

TRABAJO DE GRADO
Opción Seminario.

COMPRAYA

Corporación Universitaria Remington.
Nombre de la facultad: Ingenierías
Nombre del programa académico: Ingeniería de Sistemas

Nombres de los estudiantes autores del trabajo de grado.

Oscar Dario Peña Villamizar

Jorge Leonardo Ramírez Restrepo - docente del seminario.
Seminario
2026

Tabla de Contenidos

Resumen.....	3
Marco conceptual y normativo	4
Marco normativo.....	5
Marco contextual	10
Descripción de la organización.....	10
Problemática identificada.....	11
Identificación y análisis de activos	12
Inventario de activos	12
Análisis de amenazas y vulnerabilidades.....	18
Análisis y gestión de riesgos.....	24
Metodología de análisis	24
Matriz de riesgos	25
Políticas y controles de seguridad.....	29
Políticas propuestas.....	29
Controles propuestos.....	31
Gestión de incidentes y continuidad del negocio.....	35
Cultura organizacional en ciberseguridad.....	40
Conclusiones	43
Referencias.....	44

Resumen

CompraYa Online S.A.S. es una empresa la cual está constituida en Colombia y se centra en el comercio electrónico fue fundada hace ocho años y opera exclusivamente a través de las plataformas digitales en todo el territorio nacional esta compañía se centra en comercializar productos de tecnología, hogar, moda, deportes y de más accesorios la empresa cuenta con más de 240 colaboradores que están distribuidos en el área comercial y administrativas los cuales procesan más de seis mil quinientos pedidos de forma semanal así adquieren una bases de datos con más de ciento ochenta mil cliente

La misión está centrada en ofrecer experiencias de compra las cuales sean seguras eficientes y confiables mientras que su visión se enfoca en consolidarse como unas de las principales plataformas de comercio electrónico en el país así garantizando unos altos niveles de disponibilidad y confianza

Hablaremos de la infraestructura que lleva a CompraYa Online S.A.S decimos que la organización dispone de una infraestructura tecnológica la cual incluye más de ciento veinte computadores noventa y cinco portátiles más la plataforma web y sus sistemas CRM Y ERP

Si hablamos de los problemas identificados decimos que durante la evaluación diagnostica que se identificaron múltiples situaciones críticas en material de seguridad De la información encontramos como más relevantes usos de dispositivos personales para acceder a sistemas corporativos la ausencia de política formal de clasificación de la información, usuarios los cuales cuentan con privilegios que no corresponde a su rol y/o funciones, contraseñas que no cumplen con la complejidad mínima y por último la falta de autenticación multifactorial en los accesos administrativos

Mi propósito de este informe es diagnosticar el estado actual de la seguridad de la información y proponer un plan de mejora integral que permita a la organización fortalecer sus controles así proteger los datos de sus clientes y garantizar la continuidad operativa con el crecimiento que se proyecte

Palabras clave

- Ciberseguridad organizacional
- Políticas de seguridad
- Activos de información

- Vulnerabilidades
- Gestión de riesgos

Marco conceptual y normativo

El marco conceptual se llevara a cabo con los con los fundamentos de la seguridad de la información la cual se define como la preservación de la autenticidad, integridad, confidencialidad y la disponibilidad de información ya sea en almacenamientos como impresos o digitales, así como en aplicaciones de procesos de resiliencia operativa (EVA, 2022) (GOV, 2022) ya que tomamos la definición del decreto 338 de 2022 la cual trasciende lo meramente tecnológico para abarcar aspectos organizacionales y humanos así reconociendo que la información constituye un activos fundamental.

Con lo anterior en mente podemos hablar de la seguridad digital que por su parte es entendida como la situación de normalidad y de tranquilidad en el entorno digital atreves de apropiaciones de políticas y de buenas prácticas mediante la gestión de riesgos, el uso efectivo de las capacidades que demanda voluntad social y política de las múltiples partes interesadas (GOV, 2022) (EVA, 2022) ya que la definición resulta particularmente relevante para el entorno de nuestra empresa CompraYa Online S.A.S el cual el modelo de negocio depende enteramente del entorno digital y de la confianza de sus más de ciento ochenta mil cliente

Hablaremos de los principios de la seguridad de la información con los respectivos estándares la ISO/IEC 27001 y el modelo de seguridad y privacidad de la información los cuales establecen los principios fundamentales

- Autenticidad la cual nos garantiza la identidad de los usuarios y los sistemas participantes
- Confidencialidad es la que se encarga de asegurar que solo quienes están autorizados puedan acceder a la información
- No repudio nos dice que las acciones realizadas dentro de los sistemas deben quedar registradas de manera verificable
- Trazabilidad habla de que toda la actividad relacionada con los activos de la información debe poder ser auditada y evidenciada
- Integridad esta garantiza que la información y sus métodos de proceso son exactos y completos
- Disponibilidad esta se encarga en dar accesos a la información asegurándose que solo los usuarios autorizados la tengan en cualquier momento

Estos principios aplican directamente a la empresa CompraYa Online ya que procesa información sensible de cliente gestionando transacciones electrónicas mediante pasarelas de pago y dependiendo de la disponibilidad continua de sus plataformas para procesar más seis mil quinientos pedidos por semana

Hablaremos de unos conceptos asociados como los es la vulnerabilidad de seguridad digital la cual se define como debilidad, atributo, o la falta de aplicación de un control que permite o nos facilita la actuación de una amenaza contra los servicios tecnológicos, infraestructura tecnológica, sistemas de información y las redes e información de la organización (EVA, 2022) (GOV, 2022) este concepto es central para poder comprender los hallazgos del diagnostico de CompraYa Online donde se identificaron múltiples vulnerabilidades como la ausencia de autenticación multifactorial, contraseñas sin los requisitos de complejidad, falta de política de clasificación de información y la ausencia de procedimiento para la gestión de incidentes

Hablaremos del riesgo de seguridad digital el cual se concibe como la combinación de amenazas y vulnerabilidades que se pueden materializar en el curso de cualquier actividad en el entorno digital afectando el logro de los objetivos económicos o sociales al alterar la confidencialidad, disponibilidad, integridad (EVA, 2022) (GOV, 2022) para nuestra organización que analizamos, como en primer evento podemos hablar de la interrupción del servicio y segundo la afectación de la reputación

Hablaremos de los activos de información el cual comprendemos como todos aquellos elementos que tiene valor para la organización y requieren protección incluyendo bases de datos, sistemas de información, infraestructura tecnológica, documentos físicos y digitales, y el conocimiento del personal según establece la norma ISO/IEC 27002 la cual dice que la gestión de activos debe incluir la identificación de responsabilidades y el uso de sistemas de clasificación de información (2011, 2011)

Y por último hablamos de los controles de seguridad que son las medidas técnicas, humanas y administrativas que se implementan para mitigar los riesgos los cuales son por parte de la ISO/IEC 207002 la cual nos proporciona directrices detalladas para noventa y tres controles de seguridad agrupados en catorce dominios incluyendo políticas de seguridad, controles de acceso, criptografía, seguridad en recursos humanos, gestión de incidentes, continuidad de negocio y las relaciones con proveedores (EALDE, 2017)

Marco normativo

Empezare con las principales leyes y decretos como lo es el decreto 338 de 2022 el cual constituye la norma más relevante en materia de seguridad digital en Colombia como adicional el titulo 21 a la parte 2 del libro 2 del decreto único 1078 de 2015, estableciendo lineamientos generales para fortalecer la gobernanza de la seguridad

digital, la identificación de infraestructuras críticas cibernéticas, la gestión de riesgos y la respuesta a incidentes de seguridad digital (GOV, 2022) (GOV.CO, 2022) (EVA, 2022) este decreto nos establece definiciones fundamentales de seguridad digital, riesgo, vulnerabilidades e incidentes y nos establece que la autoridades deben adoptar medidas técnicas, humanas y administrativas para garantizar la gobernanza de la seguridad digital (GOV, 2022)

Tabla 1. Normatividad aplicable.

<i>Norma o estándar</i>	<i>Propósito</i>	<i>Aplicabilidad en la organización</i>
-------------------------	------------------	---

Decreto 338 de 2022	Establecer lineamientos generales para fortalecer la gobernanza de la seguridad digital	Ya que la organización depende de la disponibilidad continua de sus plataformas digitales para procesar los seis mil quinientos pedidos por semana este decreto nos exige adoptar medidas técnicas humanas y administrativas para garantizar la gobernanza de la seguridad digital (GOV, 2022)
Ley 1581 de 2012	Nos regula la protección de datos personales en Colombia estableciendo principios, derechos y obligaciones para el tratamiento de información personal de los ciudadanos	Ya que CompraYa Online administra una base de más de ciento ochenta mil clientes registrados los cuales incluye información personal, historiales de compras, y datos de contacto la ley exige implementar políticas de privacidad, obtener consentimientos de los titulares, garantizar el derecho de acceso, rectificación y cancelación con procesos de medidas de seguridad para proteger la información (Mayor, 2022)
Ley 1273 de 2009	Modifica el código penal colombiano así introduciendo delitos informáticos como acceso abusivo a sistemas, interceptación ilegal de datos, daño informático y suplantación de sitios web	Decimos que la organización ha sufrido intentos de acceso no autorizados a cuentas corporativas y exposición accidental de información de clientes la ley aplica para tipificar posibles conductas delictivas y fundamentar las medidas de prevención y respuesta ante incidentes de seguridad (publica, 2009)

Ley 1341 de 2009	Organiza el marco de las TIC en Colombia así fomentando un desarrollo tecnológico seguro y regulado por el estado	Ya que siendo una empresa de comercio electrónico que opera exclusivamente mediante canales digitales, la organización debe alinearse con los respectivos lineamientos de esta ley que promueve la seguridad, confiabilidad y calidad de los servicios TIC en el país (publica, 2009)
ISO/IEC 27001:2022	Norma internacional que establece los requisitos para implementar, mantener y mejorar un sistema de gestión de seguridad de la información	Ya que la organización presenta varias brechas que un SGSI permitiría abordar sistemáticamente como lo son la gestión de accesos y privilegios, la gestión de incidentes, continuidad del negocio, relación con proveedores y gestión de activos esta certificación fortalece la confianza de los clientes y socios comerciales (DNV, 2025)

- Protección de datos personales Ley 1581 de 2012

La administración de una base de datos con más de 180.000 clientes expone a la organización a riesgos legales y reputacionales significativos. El incumplimiento de esta ley puede generar sanciones económicas por parte de la Superintendencia de Industria y Comercio (SIC), además de la pérdida de confianza de los clientes, especialmente considerando que el Evento 4 evidenció la exposición accidental de información. La ley exige la implementación de políticas de privacidad, procedimientos para atender derechos de los titulares y medidas de seguridad adecuadas (GOV, 2022)

- Gobernanza de la seguridad digital Decreto 338 de 2022

Este decreto proporciona el marco conceptual y operativo para la gestión de riesgos de seguridad digital en Colombia. Para CompraYa Online, su aplicación es crítica debido a la alta dependencia de sus plataformas digitales para generar ingresos. El decreto exige la adopción de medidas técnicas, humanas y administrativas que la organización actualmente

no tiene implementadas, como la política de clasificación de información, la gestión de incidentes y la autenticación multifactor en accesos administrativos (GOV.CO, 2022)

- Prevención de delitos informáticos Ley 1273 de 2009

Los eventos de phishing e intentos de acceso no autorizado que ha sufrido la organización demuestran la vulnerabilidad frente a amenazas externas. La ley no solo permite tipificar y sancionar estas conductas, sino que también fundamenta la necesidad de implementar controles técnicos y procedimientos de respuesta que prevengan la materialización de estos delitos. (publica, 2009)

- Estandarización internacional ISO/IEC 27001 y 27002

Las normas ISO proporcionan un enfoque sistemático y reconocido internacionalmente para gestionar la seguridad de la información. Su adopción permitiría a CompraYa Online (DNV, 2025)

- Porque la Ley 1341 de 2009

Esta ley no establece los principios para el uso de tecnologías de la información y ya que como una empresa de comercio electrónico que opera exclusivamente mediante canales digitales, la organización debe alinearse con los respectivos lineamientos de esta ley que promueve la seguridad, confiabilidad y calidad de los servicios TIC en el país (publica, 2009)

Marco contextual

Descripción de la organización

CompraYa Online S.A.S. es una empresa colombiana de comercio electrónico fundada hace ocho años, dedicada a la comercialización de productos mediante canales digitales por lo cual la organización opera exclusivamente a través de plataformas electrónicas, ofreciendo un portafolio diversificado que incluye productos de tecnología, hogar, moda, deportes y accesorios para clientes en todo el territorio nacional

Actualmente, la empresa cuenta con aproximadamente doscientos cuarenta colaboradores distribuidos en diferentes áreas funcionales: comercial, tecnológica, administrativa, logística y atención al cliente. Su estructura organizacional está conformada por una Gerencia General y direcciones especializadas en Comercio, Tecnología, Marketing Digital, Servicio al Cliente, Gestión Logística, Compras y Proveedores, Talento Humano, Contabilidad y Finanzas, y Analítica de Datos

El volumen de operaciones de la organización es significativo: procesa en promedio seis mil quinientos pedidos por semana y administra una base de datos superior a ciento ochenta mil clientes registrados este crecimiento durante los últimos años ha sido impulsado por el incremento de las compras digitales y el fortalecimiento de sus plataformas tecnológicas

La infraestructura tecnológica de CompraYa Online es robusta y comprende 120 computadores de escritorio y 95 portátiles. A nivel de sistemas, cuenta con plataforma web de comercio electrónico, aplicación móvil para clientes, plataforma CRM para gestión de relaciones con clientes, sistema ERP para la administración integral del negocio, sistema de gestión de inventarios, pasarela de pagos electrónicos, sistema de gestión logística, infraestructura en nube pública, base de datos centralizada de clientes, plataforma de marketing digital, correo electrónico corporativo, sistema de respaldo de información, redes Wifi corporativas y sistema de monitoreo de infraestructura

El área tecnológica está integrada por un director de Tecnología, cuatro desarrolladores, dos administradores de infraestructura, dos analistas de soporte y un analista de bases de datos, lo que demuestra la importancia que la organización otorga a su componente tecnológico

La misión de la organización se centra en ofrecer una experiencia de compra digital segura, eficiente y confiable mediante el uso de tecnología, innovación y excelencia en el servicio al cliente. Su visión busca consolidarse como una de las principales plataformas de comercio electrónico del país, garantizando altos niveles de disponibilidad, confianza y protección de la información

Problemática identificada

Durante la evaluación realizada por una firma consultora especializada, se identificaron múltiples situaciones que evidencian debilidades significativas en la gestión de la seguridad de la información de CompraYa Online S.A.S. Estas problemáticas se agrupan en varias categorías que ameritan atención prioritaria

Como lo es las vulnerabilidades en gestión de accesos ya que Se detectó que algunos colaboradores utilizan dispositivos personales para acceder a sistemas corporativos sin controles adecuados. Adicionalmente, varios usuarios mantienen privilegios superiores a los requeridos por sus funciones actuales, lo que incrementa el riesgo de acceso indebido a información sensible ya que las contraseñas de sistemas críticos no cuentan con requisitos mínimos de complejidad y no todos los accesos administrativos utilizan autenticación multifactor es una debilidad critica ya se considera que la organización ha sufrido intentos de acceso no autorizado

Como también lo es deficiencias en gobierno y políticas de información la cual nos dice que la organización carece de una política formal de clasificación de la información, lo que genera que diferentes áreas almacenen información sensible sin criterios homogéneos de protección así también siendo inexistente un inventario actualizado de activos de información, lo que dificulta identificar qué información requiere protección prioritaria

Como lo es la gestión de incidentes y continuidad que no habla de que no existen un procedimiento formal para la gestión de incidentes de ciberseguridad. Aunque los respaldos se realizan diariamente, no se realizan pruebas periódicas de restauración, lo que pone en riesgo la capacidad de recuperación ante un desastre

También encontramos Problemáticas con las relaciones con terceros ya que se identificaron integraciones con terceros que no han sido evaluadas recientemente desde la perspectiva de seguridad, y algunos colaboradores utilizan herramientas externas no autorizadas para compartir información laboral

Hablamos de los incidentes ocurridos ya que en los últimos tres años, la organización ha enfrentado cinco incidentes relevantes: una interrupción de la plataforma web por sobrecarga durante una campaña promocional; un ataque de phishing que derivó en intentos de acceso no autorizado; fallas en la aplicación móvil por actualización incorrecta; exposición accidental de información de clientes por configuración incorrecta en la nube; y vulnerabilidades en integración con proveedor externo que afectaron procesos operativos

Y por último hablaremos de las proyecciones futuras La organización planea expandir operaciones a otros países de Latinoamérica, implementar herramientas de inteligencia artificial y fortalecer procesos de gobierno de datos. Adicionalmente, se prevé un crecimiento acelerado en la cantidad de clientes, lo que incrementará los riesgos si no se abordan las debilidades actuales

Identificación y análisis de activos

Inventario de activos

Ya que para CompraYa Online S.A.S los activos de i formación representan el recurso más valioso para su respectiva operación ya que siendo su modelo de negocio depende enteramente del procesamiento, almacenamiento y protección de datos

Tabla 2. Inventario de activos

<i>Activo</i>	<i>Tipo</i>	<i>Descripción</i>	<i>Criticidad</i>
---------------	-------------	--------------------	-------------------

Base de datos de cliente	Información	Registro de más de 180.000 clientes con datos personales, historial de compras, preferencias y datos de contacto. Constituye el principal activo de información de la organización	Crítica
Plataforma web de comercio electrónico	Tecnológico/Sistema	Sitio web principal donde los clientes realizan compras. Procesa 6.500 pedidos semanales y es el canal de ingresos más importante	Crítica
Aplicación móvil	Tecnológico/Sistema	Plataforma para dispositivos móviles que permite a los clientes realizar compras desde sus teléfonos. Canal estratégico en crecimiento	Alta
Pasarela de pagos electrónicos	Tecnológico/Sistema	Sistema que procesa transacciones electrónicas con tarjetas de crédito, débito y otros medios de pago	Crítica
Sistema ERP	Tecnológico/Sistema	Plataforma integral que gestiona recursos, compras, finanzas y proveedores	Alta

Sistema CRM	Tecnológico/Sistema	Gestiona relaciones con clientes, historial de interacciones y programas de fidelización	Alta
Sistema de gestión de inventarios	Tecnológico/Sistema	Controla existencias de productos, entradas y salidas de almacén	Alta
Sistema de gestión logística	Tecnológico/Sistema	Coordina almacenamiento, preparación, despacho y seguimiento de pedidos	Alta
Infraestructura en nube pública	Tecnológico/Infraestructura	Servidores y servicios alojados en la nube que soportan todas las plataformas y sistemas de la organización	Crítica
Correo electrónico corporativo	Tecnológico/Sistema	Medio de comunicación oficial para colaboradores y clientes	Media

Sistema de respaldo de información	Tecnológico/Sistema	Sistema que realiza copias de seguridad diarias de la información crítica	Alta
Plataforma de marketing digital	Tecnológico/Sistema	Administra campañas publicitarias, promociones y estrategias de fidelización	Media
Equipos de cómputo	Tecnológico/Infraestructura	Recursos de hardware utilizados por los 240 colaboradores para sus funciones diarias	Media
Sistema de monitoreo de infraestructura	Tecnológico/Sistema	Herramienta que supervisa el estado de la infraestructura tecnológica y detecta fallos	Media
Redes Wifi corporativas	Tecnológico/Infraestructura	Redes de comunicación interna que permiten la conectividad de dispositivos	Media
Información de proveedores	Información	Datos de proveedores, contratos, acuerdos comerciales y condiciones de servicio	Alta
Información financiera y contable	Información	Registros contables, estados financieros, presupuestos y transacciones	Alta

Propiedad intelectual	Información	Código fuente de la plataforma web, aplicación móvil y sistemas desarrollados internamente	Alta
Talento humano	Humano	Los 240 colaboradores con su conocimiento, experiencia y habilidades técnicas y comerciales	Crítica
Información de campañas y estrategias comerciales	Información	Planes de marketing, promociones, ofertas y estrategias de fidelización	Media

Justificación de los activos más importantes

- Base de datos de los clientes Nivel critico

Este es el activo más valioso de la organización por varias razones. En primer lugar, contiene información personal de más de ciento ochenta mil clientes, incluyendo datos de contacto, historial de compras y preferencias de consumo. La pérdida o exposición de esta información no solo implicaría graves sanciones legales bajo la Ley 1581 de 2012, sino también la pérdida de confianza de los clientes, lo que afectaría directamente los ingresos de la empresa

- La plataforma web Nivel critico

Es el canal principal de generación de ingresos, procesando seis mil quinientos pedidos por semana. Su indisponibilidad, como ocurrió en el Evento 1 durante una campaña promocional, no solo genera pérdidas económicas directas por ventas no realizadas, sino que también daña la reputación de la marca y la confianza de los clientes

- La pasarela de pagos electrónicos Nivel critico

Este sistema llega a falla ya que maneja información financiera extremadamente sensible, incluyendo datos de tarjetas de crédito y transacciones electrónicas. Una vulnerabilidad

en este activo podría resultar en fraudes financieros, pérdidas económicas y graves consecuencias legales

- El talento humano

Los doscientos cuarenta colaboradores son el motor de la organización. Su conocimiento, experiencia y habilidades técnicas y comerciales son irremplazables

- La propiedad intelectual o código fuente

El código fuente de la plataforma web y la aplicación móvil representa la innovación y diferenciación competitiva de la organización. Su pérdida o robo podría permitir a competidores replicar sus funcionalidades o explotar vulnerabilidades

En mi análisis de criticidad me he basado en tres factores principales para determinar su nivel que son:

- Impacto en la operación
- Sensibilidad de la información
- Dependencia de otros activos

Con esto en mente he calificado como críticos los que son cuya falla o compromiso paralizaría la operación de la organización generando pérdidas económicas significativas o afectarían gravemente la confianza del cliente lo que califique como altos son aquellos que, aunque son importantes tienen un impacto menor en términos de continuidad o sensibilidad o al menos cuentan con algún plan alternativo

Analisis de amenazas y vulnerabilidades*Tabla 3. Amenazas y vulnerabilidades*

<i>Activo</i>	<i>Amenaza</i>	<i>Vulnerabilidad</i>
---------------	----------------	-----------------------

Integraciones con terceros	Accesos que no están autorizados a través de los proveedores	Gestionar el riesgo en relación en que los proveedores son insuficientes
Integraciones con terceros	Son vulnerabilidades en sistemas de proveedores	Como lo son las integraciones no evaluadas la confianza excesiva en los servicios externos
Talento humano	Retiro de personal con conocimientos críticos	Es la ausencia de planes de sucesión o dependencia de conocimiento individual
Talento humano	Errores humanos que comprometen la seguridad de la compañía	Se debe generar una cultura que considere la seguridad como responsabilidad exclusiva de TI
Equipos de cómputo y dispositivos	Infecciones por parte de malwares o virus	Esto se debe por la falta de campañas de sensibilización a los colaboradores sobre estos riesgos

Equipos de cómputo y dispositivos	Perdida o el robo de estos dispositivos con información sensible de la compañía	Estos dispositivos personales son usados para acceder a sistemas corporativos sin controles
Sistema de respaldo de información	Perdidas de información mediante fallas en las restauraciones	No se generan pruebas de manera periódica para saber si los respaldos funcionan correctamente
Correo electrónico corporativo	Filtración de información confidencial	El uso de herramientas externas no autorizadas para compartir información laboral
Correo electrónico corporativo	Phishing y ataques de ingeniería social	Colaboradores que desconocen riesgos ya que no ahí campañas periódicas de sensibilización
Sistema ERP y CRM	Son accesos indebidos a información financiera y de clientes	Se debe a usuarios con privilegios superiores a los requeridos por funciones actuales
Infraestructura en nube pública	La interrupción del servicio por fallas del proveedor	Es la dependencia critica de un solo proveedor de nube

Infraestructura en nube pública	se debe a la exposición de datos por una configuración incorrecta	Es la falta de políticas de configuración segura y la ausencia de revisiones periódicas
Aplicación móvil	Es por fallas operativas debido a actualizaciones incorrectas	Se da por procedimientos de pruebas insuficientes
Pasarela de pagos electrónicos	El acceso no autorizado a transacciones	Son accesos administrativos sin MFA
Pasarela de pagos electrónicos	Interceptación de datos financieros	Es la integración con terceros no evaluados desde la perspectiva de seguridad y de la confianza excesiva en servicios externos
Plataforma web de comercio electrónico	La suplantación de identidad	De debe a colaboradores sin sensibilización en ciberseguridad
Plataforma web de comercio electrónico	La explotación de vulnerabilidades en el código	También se debe a la integración con terceros no evaluadas de forma reciente

Plataforma web de comercio electrónico	Ataques DDoS	Se da por una mala infraestructura en nube publica sin evolución de capacidad ante picos de sobre demanda
Base de datos de clientes	Con ataques de Ransomware que encripten la información	Se debe a respaldos diarios sin pruebas periódicas de restauración
Base de datos de clientes	Fuga o filtración de datos	Se da por almacenamientos de información sensible sin criterios homogéneos de protección
Base de datos de clientes	Los accesos no autorizados a la información del personal o clientes	Se da por la ausencia de autenticación multifactor en los accesos administrativos

Se realiza un análisis de las situaciones de mayor riesgo

- Como lo es la exposición de datos de clientes

La cual es la situación que representa el mayor riesgo para CompraYa Online es la posible exposición de los datos de sus más de ciento ochenta mil clientes ya que las vulnerabilidades que facilitan este riesgo son múltiples: ausencia de MFA, contraseñas débiles, privilegios excesivos, falta de política de clasificación y ausencia de criterios homogéneos de protección. Las consecuencias serían devastadoras: sanciones legales bajo la Ley 1581 de 2012, pérdida de confianza de clientes, daño reputacional irreparable y posible pérdida masiva de clientes hacia la competencia

- También está la indisponibilidad de la plataforma web y aplicación móvil

Ya que la plataforma web y la aplicación móvil son los canales principales de generación de ingresos ya que una sobrecarga durante una campaña promocional puede interrumpir el servicio durante varias horas, generando pérdidas económicas directas y dañando la reputación con las vulnerabilidades asociadas incluyen la falta de pruebas de capacidad

ante picos de demanda, integraciones con terceros no evaluadas y la priorización de rapidez sobre seguridad

- Podemos hablar de los ataques de phishing e ingeniería social

Se evidencia que la organización ya ha sido blanco de ataques de phishing que derivaron en intentos de acceso no autorizado a cuentas corporativas ya que la vulnerabilidad principal es la debilidad en la cultura organizacional: los colaboradores desconocen los riesgos asociados al manejo de información, no existen campañas periódicas de sensibilización, y muchos empleados consideran que la seguridad es responsabilidad exclusiva del área tecnológica un respectivo ataque que sea exitoso podría comprometer cuentas administrativas permitiendo a los atacantes acceder a información sensible así realizando transacciones fraudulentas o realizar instalaciones de malwares en el sistema

- También podemos hablar del riesgo asociado al crecimiento proyectado

Ya que la organización planea expandir operaciones a otros países de Latinoamérica e implementar herramientas de inteligencia artificial para personalización de ofertas con este crecimiento acelerado incrementará los riesgos existentes y presentará nuevos desafíos, como el cumplimiento de normativas de protección de datos en otros países, el manejo de volúmenes mayores de información y la exposición a nuevas amenazas

En conclusión, las situaciones que representan mayor riesgo son aquellas que: 1 comprometen la confidencialidad de los datos de clientes con consecuencias legales y reputacionales graves; 2 afectan la disponibilidad de las plataformas de generación de ingresos; 3 aprovechan las debilidades culturales y de sensibilización del talento humano; y 4 exponen a la organización a través de integraciones con terceros

Análisis y gestión de riesgos

Metodología de análisis

Para esta valoración de riesgos en CompraYa Online S.A.S se aplicará una metodología cualitativa basada en los lineamientos establecidos por la norma ISO/IEC 27001 del 2002 Y la respectiva guía ISO/IEC 31000 para la gestión de riesgos y el proceso de análisis considero que los activos de la información, identificados en la tabla dos las amenazas y vulnerabilidades documentadas en la tabla tres y con el contexto operativo de la organización

Las valoraciones del impacto se realizaron considerando cuatro criterios muy fundamentales que afectan a la organización

- El impacto operacional que es el grado de afectación a la capacidad de la organización para procesar los seis mil quinientos pedidos y así poder atender a sus clientes
- El impacto financiero el cual verifica las pérdidas económicas directas e indirectas derivadas de la materialización del riesgo
- El impacto legal y regulatorio el cual sanciona, multa y genera consecuencias legales conforme a la ley 1581 de 2012 y demás normas aplicables
- El impacto reputacional

Ya que cada uno de estos criterios fue calificado en una escala del 1 al 5 donde 1 nos representa un impacto menor y el 5 un impacto catastrófico el impacto total se determinó como el promedio ponderado de los cuatro criterios

Y la probabilidad de evaluó considerando estos 3

- La frecuencia de ocurrencia la cual nos da la historia de incidente previos en la organización en el sector
- El nivel de exposición el cual es el grado de exposición del activo a la amenaza considerando las vulnerabilidades existentes
- Y la efectividad de los controles actuales la cual determina las evaluaciones de las medidas de seguridad implementadas

Esta probabilidad también fue calificada según la escala del 1 al 5 donde 1 es muy improbable, 2 es improbable, 3 es posible, 4 es probable y 5 es muy probable

Con esto en mente la metodología nos permite priorizar los riesgos de manera objetiva y asignar recursos de manera eficiente a las áreas de mayor vulnerabilidad

Matriz de riesgos*Tabla 4. Matriz de riesgos*

<i>Riesgo</i>	<i>Impacto</i>	<i>Probabilidad</i>	<i>Nivel</i>
---------------	----------------	---------------------	--------------

Exposición o filtración de datos personales de clientes	5	4	20, critico
Indisponibilidad de la plataforma web y aplicación móvil	5	4	20, critico
Ataque de Ransomware que encripte información crítica	5	3	15, alto
Acceso no autorizado a cuentas administrativas	4	4	16, critico
Vulnerabilidades en integraciones con terceros	4	4	16, critico
Pérdida de información por fallas en respaldos o restauración	5	3	15, alto
Ataques de phishing e ingeniería social exitosos	4	5	20, critico
Interrupción del servicio por fallas del proveedor de nube	4	3	12, alto

Filtración de información confidencial por uso de herramientas no autorizadas	3	4	12, alto
Incidentes de seguridad no reportados oportunamente	4	4	16, critico
Robo o pérdida de dispositivos con información sensible	3	3	9, medio
Incumplimiento normative	5	3	15, alto
Explotación de vulnerabilidades en código de plataformas	4	3	12, alto
Afectación de procesos operativos por vulnerabilidades de proveedores	3	3	9, medio

Se realizará el análisis de riesgos prioritarios

- con la exposición o filtración de datos personales de clientes el cual es un riesgo que representa la mayor amenaza para la organización debido a las graves consecuencias legales, financieras y reputacionales. La base de datos de ciento ochenta mil clientes contiene información personal sensible que, si se ve expuesta, generaría sanciones por parte de la Superintendencia de Industria y Comercio conforme a la Ley 1581 de 2012, pérdida masiva de confianza de los clientes y daño reputacional irreparable (GOV, 2022)
- hablaremos de la indisponibilidad de la plataforma web y aplicación móvil ya que son los canales exclusivos de generación de ingresos y una interrupción

prolongada generaría pérdidas económicas directas como ventas no realizadas, daño a la reputación y pérdida de clientes hacia la competencia. La dependencia crítica de estos canales, sumada a la sobrecarga durante picos de demanda y la falta de pruebas de capacidad, hace que este riesgo sea crítico (carrillo, 2022)

- También Podemos hablar de los ataques de phishing e ingeniería social exitoso ya que este riesgo tiene la probabilidad más alta (5) debido a la debilidad cultural identificada: colaboradores sin sensibilización, desconocimiento de riesgos, y la percepción de que la seguridad es responsabilidad exclusiva de TI ya visto en eventos anteriores se confirmó que la organización ya ha sido blanco de ataques de phishing. Un ataque exitoso podría comprometer cuentas administrativas, permitir el acceso a información sensible, o facilitar la instalación de malware (point, 2025)
- Para los riesgos de nivel medios se dejó calificado como medios ya que casi siempre son robos de dispositivos y afectación por vulnerabilidades de proveedores estos solo requieren de monitoreo y acciones planificadas lo cual no representan una amenaza inmediata para la continuidad del negocio
- Para los riesgos alto los cuales incluyen ataque de Ransomware que encriptan información crítica o pérdida de información por fallas, aunque no requieran de acciones inmediatas como los críticos deben ser abordados en el corto plazo como medidas preventivas y correctivas

Políticas y controles de seguridad

Políticas propuestas

Tabla 5. Políticas de seguridad

<i>Política</i>	<i>Objetivo</i>	<i>Riesgo asociado</i>
-----------------	-----------------	------------------------

Política de control de accesos	Definirá los requisitos mínimos para gestionar las identidades y accesos así incluyendo la autenticación de multifactor y la revisión periódica de los privilegios otorgados	Este riesgo nos lleva a accesos no autorizados a cuentas administrativas así exponiendo datos personales ya que los usuarios tienen privilegios que no son requeridos a su cargo
Política de clasificación de la información	La cual establece criterios homogéneos para clasificar la información según su nivel de sensibilidad definiendo así medidas de protección específicas para cada categoría	Una exposición o filtración de datos personales de clientes
Política de seguridad en relación con terceros	Esta nos establece requisitos de seguridad para la contratación y evaluación periódicas de proveedores y socios comerciales así incluyendo análisis de riesgos con sus cláusulas de seguridad en contratos y auditorías	La vulnerabilidad en integraciones con terceros es la confianza excesiva en servicios externos y dependencia de proveedores
Políticas de seguridad en desarrollo de software	Esta política nos establece prácticas de desarrollo seguro la cual incluye el análisis de vulnerabilidades, pruebas de seguridad, revisión de código y control de cambios	La falla es usualmente en aplicaciones móviles por actualizaciones incorrectas las cuales casi siempre son para darle prioridad a la rapidez sobre la seguridad

	antes de subirlo a producción	
Política en gestión de dispositivos y uso aceptable	Con esta política estableceremos reglas para el uso de dispositivos personales	Ya que el uso de dispositivos personales sin control se traduce a la extracción de información laboral no autorizada

Controles propuestos

Tabla 6. Controles de seguridad

<i>Riesgo</i>	<i>Control</i>	<i>Justificación</i>
----------------------	-----------------------	-----------------------------

La exposición o filtración de datos personales de los clientes	Implementar la autenticación multifactor de manera obligatoria para todos los accesos administrativos	El MFA nos añade una capa adicional de seguridad más allá de las contraseñas así reduciendo significativamente el riesgo de acceso no autorizado incluso si las credenciales son comprometidas
La exposición o filtración de datos personales de los clientes	Nos establece políticas de clasificación de información y etiquetado de datos según su nivel de sensibilidad	Permitiendo aplicar controles de protección diferenciados según la criticidad de la información asegurando que los datos más sensibles reciban el máximo nivel de protección
Indisponibilidad de la plataforma web y el aplicativo móvil	Realizar pruebas de carga y capacidad para simular picos de demanda durante campañas promocionales	Nos permitirá identificar y corregir cuellos de botella antes de que ocurran o interrupciones reales garantizando la disponibilidad durante eventos de alto tráfico
Indisponibilidad de la plataforma web y el aplicativo móvil	Nos establece una arquitectura redundante y balanceada de carga en la infraestructura en la nube	Nos disminuirá el tráfico entre múltiples servidores asegurando que la falla de uno no afecte la disponibilidad del servicio y permitiendo escalar automáticamente ante picos de demanda
Ataques de phishing e ingeniería social	Nos implementa filtros de anti-phishing y sistemas de seguridad en el correo electrónico corporativo	Bloqueara automáticamente correos maliciosos antes de que lleguen a los colaboradores reduciendo la exposición a amenazas y complementando las

		capacitaciones sobre la ISO/IEC 27002
Acceso no autorizado a cuentas administrativas	Se implementa políticas de contraseñas robustas con requisitos de longitud, complejidad y rotación periódica	Nos establece un requisito mínimo que dificulte los ataques de fuerza bruta y adivinación de contraseñas
Vulnerabilidad en integración con terceros	Establecer un proceso formal de evaluación de seguridad de proveedores antes de la contratación y de forma periódica	Permitirá identificar y mitigar riesgos asociados a integraciones con terceros antes de que se materialicen
Perdida de información por falla en los respaldos	Se debe implementar pruebas periódicas de restauración de respaldos con registro de resultados	Nos asegura que los respaldos sean efectivos y que la organización pueda recuperar la información en caso de un desastre
Fallas en aplicaciones móviles por actualizaciones incorrectas	Establece un procedimiento de despliegue con validación previa en entornos de pruebas y con una aprobación formal	Esta nos asegura que los cambios pasen por pruebas rigurosas en un entorno separado antes de ser desplegados a producción

Justificación de las políticas y los controles para la disminución de riesgos esta políticas y controles son propuestos y constituyen un sistema integral de gestión de seguridad que aborda las debilidades identificadas en CompraYa Online S.A.S desde múltiples frentes

Ya que las políticas y los controles que fueron propuestos están alineados con los estándares ISO/IEC 27001 y 27002 lo que nos asegura que siguen unas buenas prácticas reconocidas internacionalmente

Así reduciendo los siguientes riesgos clave

- Exposición de datos de clientes
- Indisponibilidad de plataformas
- Phishing e ingeniería social
- Acceso no autorizado
- Vulnerabilidades en terceros

Con la implementación gradual y priorizada de estas políticas y controles más específico empezando por los riesgos críticos permitirá a CompraYa Online S.A.S fortalecer significativamente su postura de seguridad y preparase para su expansión regional

Gestión de incidentes y continuidad del negocio

Tabla 7. Incidentes potenciales

<i>Incidente</i>	<i>Descripción</i>	<i>Impacto</i>
Exposición o filtración masiva de datos de clientes	El acceso no autorizado o una configuración incorrecta que expone información personal de la base de datos de ciento ochenta mil clientes	El impacto es crítico ya que conlleva a sanciones legales según la ley 1581 del 2012 con la pérdida de confianza de cliente daño reputacional irreversible posible quiebra del negocio
Indisponibilidad prolongada de la plataforma web y aplicación móvil	Es la interrupción del servicio por más de 24 horas debido a ataque DDoS o la sobre carga durante campañas promocionales	Impacto critico ya que genera pérdidas económicas por ventas no realizadas de los más de seis mil quinientos pedidos semanales
Ataque de Ransomware	El cual es un cifrado de información crítica como lo es la base de datos de cliente los sistemas ERP Y CRM	El impacto es crítico ya que paraliza totalmente las operaciones con la perdida de información
Vulnerabilidad critica en integración con proveedores de pagos	Es la explotación de vulnerabilidades en la pasarela de pagos que permite interceptación de transacciones o acceso a datos financieros	El impacto es alto ya que el fraude financiero, perdida de dinero de los clientes, sanciones de entidades financieras, pérdida de confianza en el sistema de pagos

Tabla 8. Plan básico de respuesta

<i>Fase</i>	<i>Acción</i>
-------------	---------------

La preparación

- Establecer un equipo de repuestas a incidentes con roles y responsabilidades definidas
- Se documenta procedimiento de repuestas para cada tipo de incidente
- Implementación de herramientas de monitoreo y detección
- Realizar simulacros periódicos de repuestas a incidentes
- Establecer los canales de comunicación internos y externos

Detección y análisis

- Se activará el sistema de monitoreo para identificar actividades anómalas
- Se reciben registros y reportes de incidentes a través de canales establecidos
- También se evalúa el alcance del impacto y gravedad de incidente
- Notificara al equipo de repuestas y a la alta dirección según el nivel de criticidad

Contención

- Nos aísla los sistemas o segmentos afectados para evitar propagaciones
 - Desconecta los equipos comprometidos de la red
 - Se cambian las credenciales de acceso comprometidas
 - Preservara la evidencia para análisis forenses
-

Erradicación	• Eliminar la causa raíz del incidente • Se limpiará los sistemas afectados y restaurar desde los respaldos confiables • Fortalecer los controles que permiten el incidente • Se debe verificar que todos los sistemas estén limpios antes de realizar la restauración
Recuperación	• Restaurar sistemas y los datos desde respaldos verificados • Activar los planes de continuidad y contingencia según el incidente • Monitorear sistemas recuperados para confirmar operatividad normal • Se deben realizar pruebas de funcionalidad antes de reanudar operaciones completas
Lesiones aprendidas y mejora	• Se realizan reuniones de lecciones aprendidas con el equipo involucrado • Se debe documentar el incidente detalladamente • Identificar las mejoras en controles, procedimientos y capacitaciones • Actualizar el plan de respuestas con base en la experiencia • Y por último reportar a la alta dirección y a entes regulatorios según corresponda

Comunicación

- Informar a clientes afectados según nivel de incidente y normativa
 - Se usa para comunicar a entes de control
 - Gestionar la comunicación externa para proteger la reputación
 - Designar un portavoz oficial para evitar mensajes contradictorios
-

Se analiza la gestión de incidente y continuidad operativa

- Como estructura de repuesta organizada

La organización debe establecer un equipo de repuestas a incidentes el cual se conforma por el personal del área tecnológica, legal, comunicaciones y alta dirección este equipo será el responsable de activar los procedimientos según la criticidad del incidente y coordinará las acciones de repuesta

La priorización será según la criticidad

- Incidentes críticos
- Incidentes alto
- Incidentes medios

La continuidad operativa durante incidentes se basará en

- Plan de continuidad para plataformas web y aplicación móvil
- Plan de recuperación ante desastres
- Plan de contingencias para pasarela de pagos
- Plan de comunicación de crisis

Gestión de proveedores y terceros la cual dada la dependencia critica de proveedores externos la organización debe

- Establecer los acuerdos de nivel de servicio
- Contar con un proveedor alternativo
- Realizar evaluaciones periódicas de la capacidad de los proveedores

Cumplimiento normativo según la gestión de incidentes la cual considera obligación legal

Cultura organizacional en ciberseguridad

Tabla 9. Hallazgos organizacionales

<i>Situación observada</i>	<i>Riesgo asociado</i>
Muchos empleados consideran que la seguridad es responsabilidad exclusiva del área tecnológica	Ausencia de responsabilidad compartida, falta de adopción de buenas prácticas por parte de todas las áreas, vulnerabilidad ante ataques de ingeniería social
Algunas áreas priorizan la rapidez de implementación sobre la revisión de riesgos de seguridad	Despliegue de cambios sin evaluar impactos en seguridad, vulnerabilidades en producción, fallas operativas
Existe confianza excesiva en servicios externos y plataformas de terceros	Delegación de responsabilidad de seguridad sin controles, vulnerabilidades en integraciones
Algunos colaboradores desconocen los riesgos asociados al manejo de datos personales de clientes	Manejo inadecuado de información sensible, exposición accidental de datos, incumplimiento de la Ley 1581 de 2012
No todos los incidentes son reportados oportunamente	Propagación de incidentes, imposibilidad de respuesta temprana; agravamiento de consecuencias, pérdida de oportunidad de aprendizaje y mejora, repetición de incidentes
No se realizan campañas periódicas de sensibilización en ciberseguridad	Cultura de seguridad débil, desconocimiento de riesgos y buenas prácticas, baja percepción de amenazas, vulnerabilidad ante ataques de ingeniería social

Tabla 10. Recomendaciones de mejora

<i>Hallazgo</i>	<i>Recomendación</i>
La seguridad es vista como responsabilidad exclusiva de TI	Implementar un programa de Embajadores de Seguridad con representantes de cada área que promuevan buenas prácticas y sirvan de enlace con el equipo de TI
Priorización de rapidez sobre revisión de riesgos	Establecer un proceso de gateway de seguridad obligatorio antes de cualquier implementación en producción, con checklist de revisión de riesgos y aprobación de seguridad para cambios críticos
Confianza excesiva en servicios externos	Desarrollar un programa de diligencia de los proveedores que incluya evaluación de seguridad antes de la contratación y revisiones periódicas
Capacitaciones esporádicas	Establecer un programa de formación continua con frecuencia mensual, incluyendo micro aprendizaje, simulacros, y contenido adaptado para cada área
Uso de herramientas externas no autorizadas	Se debe implementar una política de uso aceptable en herramientas de su respectivo catálogo de herramientas corporativas aprobadas y seguras

Justificación como fortalecer la cultura organizacional

Hablando de la responsabilidad exclusiva a la corresponsabilidad hace que la transformación cultural más relevante que se debe lograr en CompraYa Online S.A.S. es el paso de una visión donde "la seguridad es responsabilidad exclusiva de TI" a una cultura de corresponsabilidad en seguridad

Hablaremos de los embajadores de seguridad ya que la designación de representantes de cada área como un embajador de seguridad esto crea una red descentralizada de conocimiento que multiplica el impacto de las iniciativas de seguridad los embajadores capacitados por el equipo de TI se convertirán en referentes locales para consultas y promuevan buenas prácticas en su entorno de trabajo diario

También hablaremos de las capacitaciones esporádicas ya que la falta de sensibilización mantiene a los colaboradores en un estado de desconocimiento que los convierte en un blanco fácil o como se conoce el eslabón más débil de la cadena, las recomendaciones es realizarle simulacros de phishing, capacitarlos por cada uno de sus roles y realizarles casos prácticos con ejemplos reales, así como el uso de herramientas no autorizadas pueden llevar a los sistemas a generar fallos imprevistos

Conclusiones

Realizare el análisis de estas conclusiones de la situación en ciberseguridad a base de CompraYa Online S.A.S extraeré las conclusiones de los hallazgos más relevantes y los aprendizajes obtenidos durante el desarrollo del informe y las oportunidades de mejora

Empezare por la organización presente a una brecha critica entre su madurez tecnológica y su madurez en seguridad de la información ya que CompraYa Online S.A.S. cuenta con una infraestructura tecnológica robusta y moderna, incluyendo plataformas web y móvil, sistemas CRM, ERP, nube pública y pasarela de pagos. Sin embargo, esta sofisticación tecnológica no está acompañada de políticas, procedimientos y controles de seguridad proporcionales al nivel de riesgo que maneja, con esto nos dice que la ausencia de política formal de clasificación de información y la inexistencia de un procedimiento para la gestión de incidentes

Como segunda hablaremos de la protección de datos personales el cual es un riesgo más crítico y requiere atención inmediata por parte en la base de datos de clientes la cual constituye el activo más valioso de la organización y, simultáneamente, el de mayor exposición al riesgo, las consecuencias de una filtración masiva serían devastadoras: sanciones legales bajo la Ley 1581 del 2012, pérdida masiva de clientes, daño reputacional irreversible y posibles acciones judiciales

Como tercera hablare de la debilidad cultural o el eslabón más débil de la cadena de seguridad y el que requiere la transformación más profunda ya que el diagnostico reveló que la mayoría de los colaboradores considera que la seguridad es responsabilidad exclusiva del área tecnológica, existe resistencia a mecanismos adicionales de autenticación y no todos los incidentes son reportados oportunamente por lo tanto esta cultura de delegación y desinterés convierte a los empleados en el vector de ataque más vulnerable, especialmente ante ataques de phishing e ingeniería social que ya han afectado a la organización

Dare como cuarta la organización tiene una oportunidad estratégica para convertir la seguridad en un diferente competitivo ya que si bien el diagnóstico revela múltiples debilidades, también evidencia que CompraYa Online S.A.S. tiene la oportunidad de posicionar la seguridad como un atributo diferenciador en un mercado de comercio electrónico cada vez más competitivo con esto en mente la implementación de un Sistema de Gestión de Seguridad de la Información basado en ISO/IEC 27001, el fortalecimiento de la cultura organizacional y la adopción de prácticas de seguridad proactivas permitirían a la empresa no solo mitigar riesgos, sino también generar confianza en sus clientes y prepararse adecuadamente para su expansión a otros países de Latinoamérica

Y por ultima halaremos de la dependencia de tercero y las falta de evaluaciones de integración los cuales representan un riesgo silencioso pero de alto impacto ya que la organización confía excesivamente en servicios externos y plataformas de terceros como lo son proveedor de nube, pasarela de pagos, integraciones logísticas los cuales, sin realizar evaluaciones periódicas de seguridad, Esta dependencia crítica, sumada a la ausencia de planes de contingencia y proveedores alternativos, expone a la organización a riesgos que están fuera de su control directo

Referencias

- 2011, I. I. (01 de 10 de 2011). ScienceDirect. Obtenido de ScienceDirect:
<https://www.sciencedirect.com/topics/computer-science/information-security-management-system>
- carrillo, I. (09 de 06 de 2022). watchGuard. Obtenido de watchGuard:
<https://www.watchguard.com/br/wgrd-news/blog/ecommerce-y-los-riesgos-en-los-sistemas-de-las-empresas>
- DNV. (10 de 03 de 2025). other sectors. Obtenido de other sectors:
<https://www.dnv.es/assurance/articles/iso-27001-vs-iso-27002-the-key-differences/>
- EALDE. (09 de 07 de 2017). EALDE. Obtenido de EALDE:
<https://www.ealde.es/gestion-de-riesgos-seguridad-de-la-informacion/>
- EVA. (08 de 03 de 2022). Funcion Publica. Obtenido de Funcion Publica:
<https://www1.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866>
- GOV. (08 de 03 de 2022). Alcandia mayor. Obtenido de Alcandia mayor:
https://compilacionjuridica.shd.gov.co/compilacion/docs/decreto_0338_2022.htm#INICIO
- GOV.CO. (08 de 03 de 2022). GOV.CO. Obtenido de GOV.CO:
<https://www.dnp.gov.co/LaEntidad/subdireccion-general-prospectiva-desarrollo-nacional/direccion-desarrollo-digital/Paginas/normatividad-confianza-y-seguridad-digital.aspx>
- Mayor, A. (08 de 03 de 2022). Norma. Obtenido de Norma:
<https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?dt=S&i=121646>

point, c. (12 de 10 de 2025). check point. Obtenido de check point:

<https://www.checkpoint.com/es/cyber-hub/threat-prevention/social-engineering-attacks/social-engineering-vs-phishing/>

publica, F. (08 de 03 de 2009). EVA. Obtenido de EVA:

<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492>