Análisis de riesgos en el tratamiento de datos personales en la Cámara de Comercio Buga

Corporación Universitaria Remington
Facultad de Ingenierías
Ingeniería de Sistemas

Camilo Esteban Castaño Llanos
Tutor: Jorge Leonardo Ramírez
Seminario de Ciberseguridad Organizacional
2026

Tabla de Contenidos

Resumen 3
Palabras clave 3
Marco conceptual y contextual 4
Marco Normativo Aplicable 4
Inventario de activos críticos de información 5
Desarrollo e implementación del aprendizaje 5
Importancia Estratégica de la Ciberseguridad en la Cámara de Comercio 5
Protección de Bases de Datos Empresariales 5
Controles Técnicos de Bases de Datos 6
Riesgos en Plataformas de Registro y Trámites en Línea 6
Seguridad en Redes y Servidores Institucionales 7
Segmentación de Red 7
Monitoreo y Detección 7
Protección de Datos Personales y Empresariales 8
Implementación de Políticas de Seguridad Informática 8
Gestión de Riesgos Tecnológicos 9
Plan de Respuesta ante Incidentes de Seguridad 9
Fase 1 — Preparación 9
Fase 2 — Detección y Análisis 10
Fase 3 — Contención, Erradicación y Recuperación 10
Fase 4 — Actividades Post-Incidente 10
Prevención de Phishing, Malware y Accesos No Autorizados 10
Análisis de Caso: Vulnerabilidades en la Cámara de Comercio de Buga 11
Escenario: Campaña de Spear-Phishing y Compromiso de Credenciales 11
Escenario: experiencia personal 11
Vulnerabilidades Identificadas en el Escenario 12
Soluciones Propuestas 13
Matriz de riesgos de camara y comercio buga 13
Cultura organizacional y factor humano 14
Conclusiones 15
Referencias 16

Resumen

Este informe analiza la ciberseguridad organizacional en la Cámara de Comercio de Buga, una entidad que, por la naturaleza de su función pública, concentra información sensible de miles de empresas y comerciantes del Valle del Cauca. Como repositorio del Registro Mercantil y otros sistemas de formalización empresarial, representa un objetivo atractivo para actores maliciosos en el ciberespacio, algo que no es solo una hipótesis académica, sino una realidad que he podido constatar de forma directa.

A través de un análisis técnico, el documento examina las principales amenazas que enfrenta la entidad: phishing, ransomware, accesos no autorizados y vulnerabilidades en sus plataformas de trámites en línea. Para cada una de ellas se proponen controles, políticas y marcos de gestión de riesgos alineados con estándares como ISO/IEC 27001, el Marco NIST CSF 2.0 y la normativa colombiana vigente, especialmente la Ley 1581 de 2012 sobre protección de datos personales.

El informe también incluye un análisis de caso basado en patrones documentados en entidades similares, una experiencia personal que motivó su elaboración, una matriz de riesgos con priorización y un plan de respuesta ante incidentes. La conclusión central es que una estrategia integral de ciberseguridad no solo protege los activos de la Cámara, sino que fortalece la confianza institucional de todos quienes dependen de sus servicios.

Palabras clave

Ciberseguridad organizacional · Cámara de Comercio · Protección de datos · ISO/IEC 27001 · Gestión de riesgos · Registro mercantil · Phishing · Ransomware · Control de acceso · Plan de respuesta a incidentes · Ley 1581 de 2012 · Infraestructura crítica

Marco conceptual y contextual

La Cámara de Comercio de Guadalajara de Buga es una entidad de carácter gremial, con funciones públicas delegadas por el Estado colombiano, que ejerce su jurisdicción sobre el municipio de Buga y varios municipios aledaños del Valle del Cauca. Entre sus responsabilidades centrales se destacan: la administración del Registro Mercantil, el Registro Único de Proponentes (RUP), el Registro de Entidades sin Ánimo de Lucro (ESAL), la expedición de certificados de existencia y representación legal, y la prestación de servicios de arbitraje y conciliación (Cámara de Comercio de Buga, 2024).

Desde el proceso de transformación digital impulsado por la Confederación Colombiana de Cámaras de Comercio (Confecámaras), la entidad ha migrado gran parte de sus trámites a plataformas virtuales, lo que ha incrementado significativamente su superficie de ataque digital. Hoy, miles de transacciones que involucran datos sensibles de personas naturales y jurídicas se realizan diariamente a través de canales electrónicos, generando un imperativo categórico por la seguridad de la información (Confecámaras, 2023).

Marco Normativo Aplicable

La gestión de ciberseguridad en la Cámara de Comercio de Buga debe enmarcarse en el siguiente conjunto normativo:

- Ley 1581 de 2012 y Decreto Reglamentario 1377 de 2013: Régimen general de protección de datos personales en Colombia. Establece los principios de legalidad, finalidad, libertad, veracidad, transparencia, acceso restringido y seguridad que deben regir el tratamiento de datos.
- Ley 1273 de 2009: Tipifica los delitos informáticos en Colombia, incluyendo el acceso abusivo a sistemas informáticos, la interceptación de datos, el daño informático y la violación de datos personales.
- CONPES 3995 de 2020: Política Nacional de Confianza y Seguridad Digital, que establece la hoja de ruta del país en materia de ciberseguridad para entidades públicas y privadas.
- ISO/IEC 27001:2022: Estándar internacional para Sistemas de Gestión de Seguridad de la Información (SGSI), que proporciona los requisitos para establecer, implementar, mantener y mejorar un SGSI.
- Marco NIST CSF 2.0: Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología de EE.UU., ampliamente adoptado globalmente, organizado en seis funciones: Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar.

Inventario de activos críticos de información

Antes de realizar la matriz de riesgos se identificaron los siguientes activos críticos de información:

- Base de datos del registro mercantil
- Plataforma virtual de trámites
- Servidores institucionales
- Correos corporativos
- Datos personales de empresarios
- Equipos de funcionarios
- Sistema de certificados empresariales
- Información financiera de comerciantes

Estos activos fueron priorizados porque soportan procesos críticos y su afectación impactaría la continuidad operativa de la Cámara de Comercio de Buga.

Desarrollo e implementación del aprendizaje

Importancia Estratégica de la Ciberseguridad en la Cámara de Comercio

La Cámara de Comercio de Buga gestiona activos de información de alto valor estratégico: bases de datos con información completa de miles de empresas registradas en su jurisdicción, documentos de constitución de sociedades, poderes notariales, estados financieros y datos personales de representantes legales y socios. Una brecha de seguridad en este entorno no solo implicaría pérdidas económicas directas, sino que podría comprometer la fe pública, generar responsabilidades legales bajo la Ley 1581 y deteriorar irreversiblemente la confianza institucional (Cano, 2021).

Según el informe de amenazas de Fortinet para América Latina (2024), Colombia registró más de 14.000 millones de intentos de ciberataques en el primer semestre del año, posicionándose entre los países más atacados de la región. Las entidades del sector comercial e institucional, que procesan grandes volúmenes de datos de terceros, son objetivos prioritarios para actores de amenaza motivados por el lucro económico y el espionaje corporativo.

Protección de Bases de Datos Empresariales

Las bases de datos del Registro Mercantil constituyen el activo de información más crítico de la Cámara. Contienen no solo información de naturaleza pública, sino también datos privados y reservados de los empresarios registrados. La

protección efectiva de estas bases de datos requiere una estrategia de defensa en profundidad:

Controles Técnicos de Bases de Datos

- Cifrado en reposo mediante AES-256 para proteger los datos almacenados incluso en caso de acceso físico no autorizado al servidor.
- Cifrado en tránsito con TLS 1.3 para todas las comunicaciones entre la capa de aplicación y el motor de base de datos.
- Implementación del principio de mínimo privilegio mediante Control de Acceso Basado en Roles (RBAC), asegurando que cada funcionario acceda únicamente a los datos necesarios para su función.
- Enmascaramiento dinámico de datos (Dynamic Data Masking) para ocultar información sensible a usuarios sin autorización de visualización completa.
- Monitoreo continuo mediante herramientas de Database Activity Monitoring (DAM) que registran y alertan sobre consultas anómalas o accesos inusuales.
- Procedimientos automatizados de backup con esquema 3-2-1: tres copias, en dos medios diferentes, una almacenada fuera de las instalaciones (offsite o en la nube).

Riesgos en Plataformas de Registro y Trámites en Línea

Las plataformas virtuales de la Cámara de Comercio, a través de las cuales los ciudadanos realizan renovaciones de matrícula mercantil, consultas de certificados, inscripción de actos y trámites ante el RUP, presentan una superficie de ataque significativa que debe ser gestionada con rigor técnico.

Los vectores de ataque más frecuentes en este tipo de plataformas incluyen:

- Inyección SQL: El atacante inserta comandos SQL maliciosos en campos de entrada no validados, pudiendo leer, modificar o eliminar registros en la base de datos.
- Cross-Site Scripting (XSS): Inyección de scripts maliciosos en páginas web que afectan a los usuarios legítimos de la plataforma.
- Ataques de fuerza bruta: Intentos automatizados de adivinar credenciales de acceso mediante diccionarios de contraseñas.
- Man-in-the-Middle (MitM): Interceptación de comunicaciones entre el usuario y el servidor para robar sesiones o credenciales.
- Broken Authentication: Explotación de debilidades en los mecanismos de autenticación y gestión de sesiones.

Para mitigar estos riesgos, se recomienda implementar un Web Application Firewall (WAF), realizar análisis SAST y DAST sobre el código de la plataforma, aplicar el estándar OWASP Top 10 en el ciclo de desarrollo seguro y habilitar autenticación multifactor (MFA) para todos los usuarios con privilegios de modificación en el sistema (OWASP Foundation, 2021).

Seguridad en Redes y Servidores Institucionales

La infraestructura de red de la Cámara de Comercio de Buga debe diseñarse bajo el paradigma de Zero Trust Architecture (ZTA), donde ningún usuario o dispositivo es confiable por defecto, independientemente de si se encuentra dentro o fuera del perímetro organizacional.

Segmentación de Red

La red institucional debe segmentarse en zonas de seguridad claramente definidas mediante VLANs y firewalls internos:

- Zona DMZ (Demilitarized Zone): Para los servidores web y de aplicaciones expuestos al público.
- Zona de datos: Para los servidores de bases de datos, con acceso estrictamente restringido.
- Zona corporativa: Para las estaciones de trabajo de los funcionarios, separada de la red de visitantes.
- Zona de gestión: Para los dispositivos de administración de red, accesibles únicamente por el equipo de TI.

Monitoreo y Detección

La implementación de un sistema SIEM (Security Information and Event Management) permitirá correlacionar eventos de seguridad provenientes de múltiples fuentes en tiempo real, facilitando la detección temprana de incidentes. Complementariamente, un IDS/IPS (Intrusion Detection/Prevention System)

analizará el tráfico de red en busca de patrones de ataque conocidos y comportamientos anómalos.

Protección de Datos Personales y Empresariales

En cumplimiento de la Ley 1581 de 2012, la Cámara de Comercio de Buga está obligada a implementar las medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad de los datos personales bajo su custodia. Esto incluye la elaboración y publicación de una Política de Tratamiento de Datos Personales, el nombramiento de un Oficial de Protección de Datos (DPO), la gestión de autorizaciones de los titulares y la atención de solicitudes de acceso, rectificación, cancelación y oposición (derechos ARCO) (Congreso de la República de Colombia, 2012; Superintendencia de Industria y Comercio, 2023).

Desde una perspectiva técnica, la protección de datos personales requiere la clasificación de los activos de información según su sensibilidad, la aplicación de controles proporcionales al nivel de criticidad y el establecimiento de procedimientos claros para la notificación de brechas de seguridad ante la Superintendencia de Industria y Comercio (SIC) dentro del plazo legal establecido.

Implementación de Políticas de Seguridad Informática

Un programa robusto de ciberseguridad requiere un conjunto documentado y aprobado de políticas que establezcan las reglas y expectativas de comportamiento en materia de seguridad para todos los miembros de la organización. Para la Cámara de Comercio de Buga, se propone el siguiente conjunto de políticas prioritarias (Ministerio de Tecnologías de la Información y las Comunicaciones [MinTIC], 2020):

- Política de Seguridad de la Información: Documento marco que establece el compromiso de la Dirección con la seguridad y los principios generales del SGSI.
- Política de Uso Aceptable de Recursos Tecnológicos: Define el uso permitido de dispositivos, redes, correo electrónico e internet corporativo.
- Política de Gestión de Contraseñas: Establece requisitos de complejidad, longitud mínima (12 caracteres), caducidad y prohibición de reutilización.

- Política de Control de Acceso: Regula los procedimientos de alta, modificación y baja de usuarios en los sistemas de información.
- Política de Gestión de Incidentes de Seguridad: Define los procedimientos para la identificación, clasificación, respuesta y reporte de incidentes.
- Política de Copias de Seguridad y Recuperación: Establece la frecuencia, medios y procedimientos de restauración de backups.

Política de Teletrabajo y Acceso Remoto: Regula las condiciones de seguridad para el trabajo fuera de las instalaciones.

Gestión de Riesgos Tecnológicos

La gestión de riesgos tecnológicos es el proceso sistemático de identificar, evaluar, tratar y monitorear los riesgos que amenazan los activos de información de la organización. Para la Cámara de Comercio de Buga, se propone adoptar la metodología de gestión de riesgos establecida en la norma ISO/IEC 27005, complementada con los lineamientos del Marco NIST CSF 2.0 (International Organization for Standardization [ISO], 2022).

El ciclo de gestión de riesgos contempla las siguientes fases: (1) Establecimiento del contexto, definiendo el alcance del análisis y los criterios de aceptación del riesgo; (2) Identificación de activos de información y sus propietarios; (3) Identificación de amenazas y vulnerabilidades relevantes para cada activo; (4) Análisis del riesgo inherente mediante la fórmula Riesgo = Probabilidad × Impacto; (5) Evaluación del riesgo residual considerando los controles existentes; (6) Tratamiento del riesgo mediante aceptación, mitigación, transferencia o eliminación; y (7) Monitoreo y revisión periódica del mapa de riesgos.

Plan de Respuesta ante Incidentes de Seguridad

La Cámara de Comercio de Buga debe contar con un Plan de Respuesta ante Incidentes (PRI) documentado, probado y actualizado periódicamente. Basado en el estándar NIST SP 800-61 (National Institute of Standards and Technology [NIST], 2012), este plan debe contemplar las siguientes fases:

Fase 1 — Preparación

Establecimiento del Equipo de Respuesta ante Incidentes (CSIRT), definición de roles y responsabilidades, configuración de herramientas de monitoreo, elaboración de playbooks para los escenarios de incidente más probables (ransomware, phishing masivo, brecha de datos, DDoS) y realización de ejercicios de simulacro periódicos.

Fase 2 — Detección y Análisis

Monitoreo continuo de alertas del SIEM e IDS, causa inicial para determinar si el evento constituye un incidente real, clasificación según su gravedad (P1 crítico a P4 bajo) y notificación al responsable del área afectada y a la Dirección.

Fase 3 — Contención, Erradicación y Recuperación

Aislamiento de los sistemas comprometidos para evitar la propagación, recopilación de evidencia forense, eliminación del vector de ataque y las herramientas maliciosas, restauración de sistemas desde backups verificados y validación de la integridad de los datos recuperados.

Fase 4 — Actividades Post-Incidente

Elaboración del informe final del incidente, análisis de causa raíz, identificación de lecciones aprendidas, actualización de controles para prevenir recurrencia y notificación a autoridades competentes (SIC, Policía Nacional-DIJÍN/CAI Virtual) cuando sea procedente según la normativa vigente.

Prevención de Phishing, Malware y Accesos No Autorizados

Dado que el factor humano es frecuentemente el eslabón más débil en la cadena de seguridad, la Cámara de Comercio de Buga debe implementar un programa robusto de concienciación y formación en ciberseguridad dirigido a todos sus funcionarios. Este programa debe incluir:

- Simulaciones de phishing controladas, ejecutadas trimestralmente, para medir la susceptibilidad de los empleados y dirigir acciones de formación específicas.
- Capacitación anual obligatoria en identificación de correos maliciosos, gestión segura de contraseñas y reporte de incidentes.

- Implementación de soluciones de seguridad de correo electrónico con filtros antiphishing, análisis de sandbox para archivos adjuntos y autenticación de dominio mediante SPF, DKIM y DMARC.
- Despliegue de soluciones EDR (Endpoint Detection and Response) en todas las estaciones de trabajo para detectar y responder a comportamientos maliciosos en tiempo real.
- Gestión centralizada de identidades mediante un sistema IAM (Identity and Access Management) con soporte para MFA obligatorio en todos los sistemas críticos.

Análisis de Caso: Vulnerabilidades en la Cámara de Comercio de Buga

Para ilustrar la aplicabilidad del marco teórico expuesto, se presenta a continuación un escenario hipotético construido a partir de patrones de vulnerabilidad documentados en entidades del mismo sector, seguido de un caso de experiencia propia que motivó directamente la elaboración de este informe.

Escenario: Campaña de Spear-Phishing y Compromiso de Credenciales

En el mes de octubre de 2024, la Cámara de Comercio de Buga recibe un reporte interno de que uno de sus funcionarios del área de Registro Mercantil hizo clic en un enlace contenido en un correo electrónico que aparentaba ser una comunicación oficial de Confecámaras. El correo, redactado con un nivel de sofisticación que simulaba fielmente la identidad gráfica de la organización, dirigía al funcionario a una página de inicio de sesión falsa donde este ingresó sus credenciales corporativas.

Con las credenciales del funcionario comprometidas, el atacante accedió al sistema de gestión de registros y exportó un archivo con datos de 2.300 empresas inscritas, incluyendo información de socios, estados financieros aportados voluntariamente y datos de contacto de representantes legales. El incidente no fue detectado por los controles existentes durante 72 horas, tiempo suficiente para que la información fuera exfiltrada.

Escenario: experiencia personal

Como estudiante de Ingeniería de Sistemas y emprendedor, tengo registro activo en la Cámara de Comercio de Buga, lo que me dio una perspectiva directa sobre las vulnerabilidades que este informe busca documentar.

En el año 2022, aproximadamente quince días después de completar el proceso de inscripción de mi emprendimiento, comencé a recibir correos electrónicos fraudulentos dirigidos específicamente a mí, acompañados de llamadas telefónicas con presuntas amenazas de carácter extorsivo. Lo que más me llamó la atención no fue solo el hecho en sí, sino la precisión con la que los atacantes conocían mis datos recién registrados: nombre, actividad económica e información de contacto. Esto me llevó a concluir que la fuente del ataque estaba directamente relacionada con el proceso de registro mercantil.

Al indagar con otros emprendedores de la región, confirmé que este tipo de situaciones no es un caso aislado. Por el contrario, es un patrón recurrente que afecta a quienes formalizan sus negocios, hasta el punto de que muchos lo asumen como algo "normal" dentro del proceso de registro. Esa normalización es, en sí misma, una señal de alarma: indica que existe una vulnerabilidad estructural en el manejo de los datos de nuevos inscritos que no ha sido atendida con la seriedad que merece.

Esta experiencia fue, en gran medida, la motivación principal para desarrollar el presente informe. Considero que documentar y analizar estos riesgos desde un enfoque técnico es una forma concreta de aportar a la seguridad de otros emprendedores que, como yo, confían en la Cámara de Comercio con información sensible de sus negocios.

Vulnerabilidades Identificadas en el Escenario

- Ausencia de autenticación multifactorial (MFA) en el sistema de registro, lo que permitió al atacante acceder con solo las credenciales robadas.
- Carencia de un sistema DLP que pudiera detectar y bloquear la exportación masiva de datos inusual.
- Filtros de correo electrónico insuficientes que no detectaron los indicadores de phishing del mensaje malicioso.
- Falta de capacitación reciente del personal en identificación de técnicas de ingeniería social.
- Ausencia de alertas en el SIEM para accesos desde ubicaciones geográficas inusuales o en horarios atípicos.

Soluciones Propuestas

- Implementación inmediata de MFA basado en aplicación autenticadora (TOTP) para todos los accesos al sistema de registro.
- Despliegue de una solución DLP con reglas para detectar exportaciones masivas de registros fuera del horario laboral.
- Actualización de las reglas del filtro de correo con inteligencia de amenazas actualizada y habilitación del análisis de sandbox.
- Ejecución de un programa de concientización de emergencia con énfasis en spear-phishing y reporte inmediato de incidentes sospechosos.
- Configuración de alertas en el SIEM para logins desde IPs o ubicaciones no reconocidas y actividades de exportación masiva.

Los riesgos fueron valorados considerando la probabilidad de ocurrencia y el impacto sobre los activos críticos de información de la Cámara de Comercio de Buga. Se priorizaron aquellos eventos que podrían afectar la continuidad operativa, la protección de datos personales y la confianza institucional.

Matriz de riesgos de camara y comercio buga

La siguiente matriz presenta los principales riesgos cibernéticos identificados en la Cámara de Comercio de Buga, evaluados según su probabilidad de ocurrencia (escala 1-5) e impacto potencial (escala 1-5). El nivel de riesgo se calcula como el producto de ambas variables. La escala de clasificación es: Crítico (16-25), Alto (10-15), Medio (5-9), Bajo (1-4).

N°	Riesgo Identificado	Prob.	Impacto	Nivel (P×I)	Clasificación	Control Propuesto
1	Phishing y suplantación de identidad	5	4	**20**	**CRÍTICO**	*Autenticación multifactor, capacitación*
2	Acceso no autorizado a BD mercantil	4	5	**20**	**CRÍTICO**	*Control de acceso basado en roles (RBAC)*
3	Ransomware en servidores	3	5	**15**	**ALTO**	*Backups offsite, segmentación de red*

4	Fuga de datos personales (Ley 1581)	4	4	**16**	**ALTO**	*Cifrado AES-256, DLP, auditorías*
5	Ataques DDoS a plataformas online	3	4	**12**	**ALTO**	*CDN, WAF, rate limiting*
6	Vulnerabilidades en software desactualizado	4	3	**12**	**ALTO**	*Gestión de parches, pentesting*
7	Ingeniería social a funcionarios	3	3	**9**	**MEDIO**	*Formación continua, simulacros*
8	Intercepción de comunicaciones	2	4	**8**	**MEDIO**	*VPN, TLS 1.3, correo cifrado*
9	Malware en dispositivos USB	3	3	**9**	**MEDIO**	*Política de dispositivos, endpoint protection*
10	Pérdida de disponibilidad de servicios	2	3	**6**	**BAJO**	*Plan de continuidad, redundancia*

Cultura organizacional y factor humano

A lo largo de la elaboración de este informe, una conclusión se fue haciendo cada vez más evidente: los sistemas más robustos pueden fallar si las personas que los usan no están preparadas para reconocer una amenaza. En la Cámara de Comercio de Buga, como en la mayoría de organizaciones, el factor humano sigue siendo el eslabón más vulnerable de la cadena de seguridad.

Abrir un correo sospechoso, compartir una contraseña con un compañero por comodidad, o no reportar un comportamiento extraño en el sistema porque "no parece tan grave": estas acciones, aparentemente menores, son precisamente las que abren la puerta a ataques como el phishing y la fuga de información. El informe de Verizon (2024) confirma que la gran mayoría de las brechas de seguridad documentadas a nivel global tienen al factor humano como punto de entrada.

Por eso, más allá de los controles técnicos, es indispensable construir una cultura organizacional donde la seguridad de la información sea responsabilidad de todos, no solo del área de TI. Para lograrlo, se recomienda implementar capacitaciones trimestrales con casos prácticos y actualizados, simulaciones de phishing controladas que permitan medir la preparación real del personal, y campañas permanentes de concientización adaptadas al lenguaje y contexto de los funcionarios de la entidad.

La tecnología protege, pero son las personas quienes deciden si esa protección funciona o no.

Conclusiones

Desarrollar este informe me permitió no solo ordenar los conocimientos adquiridos durante el seminario, sino también conectarlos con una realidad que viví de manera directa como emprendedor registrado en la Cámara de Comercio de Buga. Las siguientes conclusiones recogen los hallazgos más importantes:

Primera: La Cámara de Comercio de Buga opera como una infraestructura de información crítica para el tejido empresarial del centro del Valle del Cauca. La digitalización progresiva de sus trámites ha ampliado significativamente su superficie de ataque, lo que hace indispensable un enfoque estructurado y proactivo de ciberseguridad organizacional. No es una opción, es una necesidad urgente.

Segunda: Los riesgos de mayor criticidad identificados, el phishing dirigido y el acceso no autorizado a la base de datos del Registro Mercantil, requieren acciones de mitigación inmediatas. La autenticación multifactorial, las soluciones DLP y los programas de concienciación para el personal son controles de implementación relativamente sencilla que pueden reducir drásticamente la probabilidad de que estos escenarios se materialicen.

Tercera: El cumplimiento de la Ley 1581 de 2012 no es únicamente una obligación legal. Es una responsabilidad ética de la Cámara frente a los miles de empresarios y comerciantes que le confían sus datos personales y empresariales. Implementar las medidas propuestas en este informe contribuye directamente a honrar esa confianza.

Cuarta: La seguridad de la información es un proceso continuo, no un estado que se alcanza una vez y se mantiene solo. Adoptar el estándar ISO/IEC 27001 como marco de referencia para el SGSI de la Cámara permitirá un ciclo de mejora continua que adapte los controles a la evolución constante del panorama de amenazas.

Quinta: El factor humano sigue siendo el vector de ataque más explotado por los cibercriminales. Invertir en la formación y concienciación de los funcionarios no es un gasto secundario: es, posiblemente, la inversión más rentable en términos de

reducción del riesgo. Mi propia experiencia como emprendedor atacado pocas semanas después de registrarme es evidencia de ello.

Sexta: Un Plan de Respuesta ante Incidentes documentado, probado y actualizado es fundamental para garantizar la resiliencia de la institución. Su ausencia no significa que los incidentes no ocurrirán, sino que cuando ocurran, la respuesta será improvisada y los daños, mayores.

Referencias

Cámara de Comercio de Guadalajara de Buga. (2024). Servicios registrales y funciones delegadas. Cámara de Comercio de Buga. https://www.ccbuga.org.co

Cano, J. J. (2021). Ciberseguridad empresarial: Reflexiones y retos para las organizaciones colombianas. Revista de Ingeniería de la Universidad de los Andes, (52), 14-23.

Confecámaras. (2023). Informe de gestión del Sistema de Registro Empresarial en Colombia. Confederación Colombiana de Cámaras de Comercio.

Congreso de la República de Colombia. (2009). Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos". Diario Oficial N.° 47.223.

Congreso de la República de Colombia. (2012). Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial N.° 48.587.

Consejo Nacional de Política Económica y Social. (2020). CONPES 3995: Política Nacional de Confianza y Seguridad Digital. Departamento Nacional de Planeación.

Fortinet. (2024). Panorama global de amenazas 2024: Informe del primer semestre. FortiGuard Labs.

International Organization for Standardization. (2022). ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO.

International Organization for Standardization. (2022). ISO/IEC 27005:2022 — Information security, cybersecurity and privacy protection — Guidance on managing information security risks. ISO.

Ministerio de Tecnologías de la Información y las Comunicaciones. (2020). Guía de seguridad y privacidad de la información para entidades del Estado. MinTIC.

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework 2.0. U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

National Institute of Standards and Technology. (2012). NIST SP 800-61 Rev. 2: Computer Security Incident Handling Guide. U.S. Department of Commerce.

OWASP Foundation. (2021). OWASP Top Ten 2021: The ten most critical web application security risks. https://owasp.org/www-project-top-ten/

Superintendencia de Industria y Comercio. (2023). Guía para la implementación del principio de responsabilidad demostrada. SIC Colombia.

Verizon. (2024). 2024 Data Breach Investigations Report. Verizon Business. https://www.verizon.com/business/resources/reports/dbir/