LoyalShield

Manual Básico de Ciberseguridad para Ejecutivos de Nivel C

LoyalShield
SECURITY SOLUTIONS

empower your business

Manual básico de ciberseguridad.

Contenido

Manual básico de ciberseguridad

Introducción

La ciberseguridad es un componente esencial en la protección de los activos más valiosos de tu empresa. Este manual te proporcionará las definiciones clave, las mejores prácticas y estrategias que todo ejecutivo de nivel C (CEO, CMO, CFO, COO..) debe conocer para gestionar y mitigar riesgos cibernéticos de manera efectiva.

¿Sabías que 1 de cada 8 empresas en América Latina ha sufrido incidentes digitales debido a una baja inversión en ciberseguridad?

1

Términos Clave en Ciberseguridad

Hoy en día, los ejecutivos de nivel C están tomando decisiones que afectan la seguridad y estabilidad de sus organizaciones. Comprender los conceptos clave de ciberseguridad no es solo responsabilidad del equipo de TI, sino una necesidad crítica para los líderes que supervisan la dirección estratégica de la empresa.

Además, tener un conocimiento sólido de estos términos permite tomar decisiones informadas, gestionar riesgos de manera más efectiva y responder adecuadamente ante incidentes de seguridad.

1.1. Ciberseguridad

La ciberseguridad se refiere al conjunto de prácticas, tecnologías y procesos diseñados para proteger los sistemas, redes, dispositivos y datos de accesos no autorizados, ataques, daños o robos.

Para un ejecutivo de nivel C, la ciberseguridad es una cuestión estratégica que va más allá de la simple protección técnica. Se trata de gestionar el riesgo empresarial asociado con las amenazas digitales. Una estrategia de ciberseguridad robusta debe integrarse en los objetivos generales de la empresa, ayudando a asegurar la continuidad del negocio, mantener la confianza de los clientes, cumpliendo con normativas y regulaciones.

1.2. Malware

Software malicioso diseñado para infiltrarse, dañar o controlar sistemas informáticos sin el conocimiento o consentimiento del usuario.

El malware representa un riesgo financiero y operacional significativo. Asegurar que se implementen soluciones de detección y prevención de malware es esencial para proteger los activos digitales de la empresa. Los líderes deben promover políticas de seguridad que minimicen las oportunidades de infección, como actualizaciones regulares de software y capacitación en ciberseguridad para todos los colaboradores.

Tipos de Malware

Virus: Infecta archivos o programas legítimos, activándose cuando se ejecutan, y puede dañar o modificar información en el sistema.

Gusanos: Se auto-replica y se distribuye a través de redes sin intervención del usuario, lo que permite su rápida propagación.

Ransomware: Bloquea el acceso a los archivos o sistemas del usuario hasta que se paga un rescate.

Troyano: Se disfraza de software legítimo para engañar al usuario y realizar acciones maliciosas, como el robo de información o la instalación de otros malware.

Spyware: Se instala de forma oculta, monitoreando las actividades del usuario y recopilando datos confidenciales como contraseñas o información financiera.

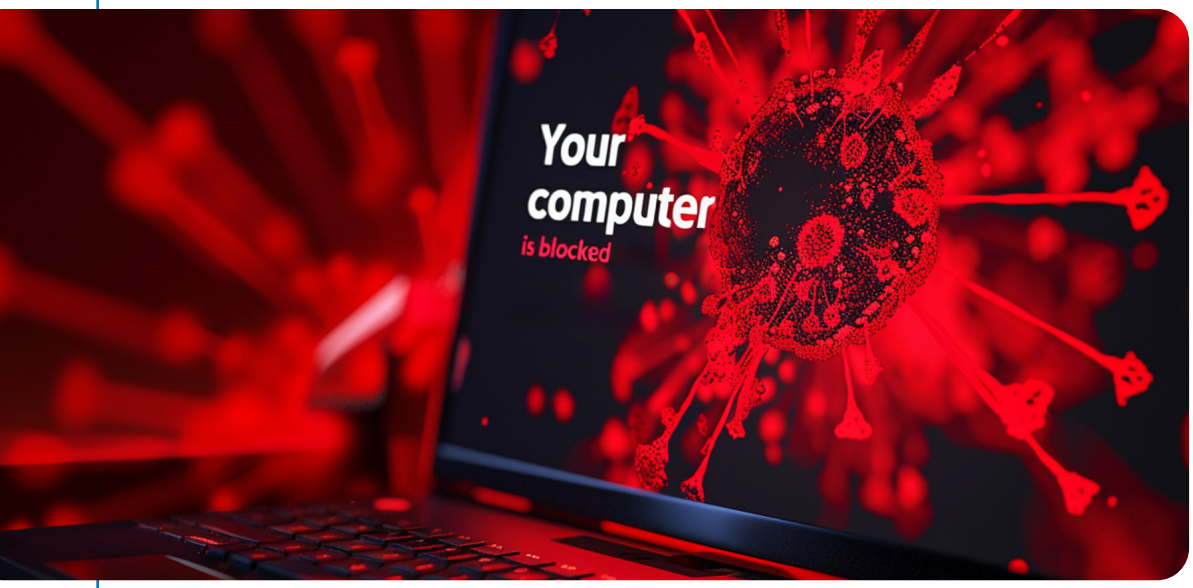
Adware: Genera anuncios no solicitados que, además de ser molestos, pueden dirigir al usuario a sitios maliciosos o comprometer la privacidad.

Rootkit: Permite a los atacantes obtener control total sobre un sistema, ocultando su presencia y la de otros programas maliciosos instalados.

Keylogger: Graba cada tecla presionada por el usuario, lo que permite a los atacantes robar información sensible como credenciales de acceso o datos bancarios.

Botnet: Consiste en una red de dispositivos infectados que pueden ser controlados remotamente para realizar ataques coordinados, como los de denegación de servicio (DDoS).

Backdoor: Crea una puerta trasera en el sistema que permite al atacante entrar en cualquier momento sin que el usuario lo sepa, eludiendo las medidas de seguridad.



1.3. Ingeniería Social

La ingeniería social es una técnica utilizada por atacantes para manipular a individuos y hacer que revelen información confidencial o realicen acciones que comprometan la seguridad de una organización.

Estos ataques se basan en la explotación de la confianza y las emociones, como el miedo, la urgencia o la curiosidad. Es fundamental entender que **estos ataques suelen ser más efectivos que los ataques puramente técnicos.** Una estafa de **phishing** bien ejecutada, por ejemplo, puede engañar a los empleados para que compartan contraseñas o información sensible.

La ingeniería social puede atacar a cualquier persona dentro de la organización, y la educación de los colaboradores es una defensa clave contra este tipo de amenazas. Como líderes, deben asegurarse de que la **cultura de la empresa fomente una mentalidad de seguridad.**

2

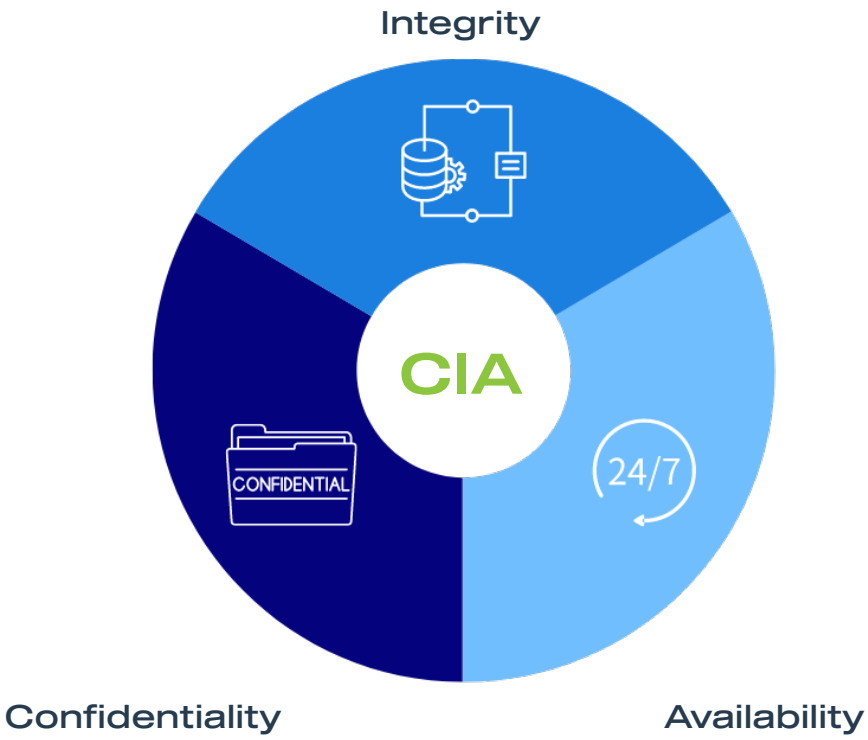
Principios Fundamentales de Ciberseguridad

Más allá de los términos técnicos, los principios fundamentales de ciberseguridad proporcionan el marco necesario para desarrollar estrategias efectivas de protección. Estos principios CIA por sus siglas en inglés (confidencialidad, integridad y disponibilidad) no solo ayudan a proteger los datos y sistemas, sino que también forman la base de cualquier política y programa de seguridad dentro de la organización.

Para los ejecutivos de nivel C, comprender estos principios es crucial, ya que la ciberseguridad no debe verse como una simple medida técnica, sino como un componente estratégico integral. La capacidad de evaluar y gestionar el riesgo, asegurar el cumplimiento normativo y establecer una cultura de seguridad dentro de la empresa comienza con un entendimiento profundo de estos fundamentos.

2.1. Triada CIA

La Triada CIA es el núcleo de cualquier política de ciberseguridad, y cada uno de sus componentes se enfoca en un aspecto específico de la protección de la información.



Confidencialidad (Confidentiality): Implica proteger la información sensible contra el acceso no autorizado. Esto no solo se refiere a evitar que terceros puedan ver o utilizar datos sin permiso, sino también a asegurar que los datos no sean revelados a colaboradores o usuarios internos sin necesidad de conocerlos.

Integridad (Integrity): Asegura que la información es precisa y completa, y que no ha sido alterada de manera no autorizada.

Disponibilidad (Availability): Garantiza que los sistemas, servicios y datos estén accesibles para los usuarios autorizados cuando los necesiten.

Recuerda que la tríada CIA ofrece una lista de verificación clara y completa para evaluar las herramientas y procedimientos de seguridad. Un sistema de seguridad efectivo cumple con estos tres principios fundamentales. Si falta uno de estos elementos, la seguridad de la información se considera insuficiente.

Además, la tríada CIA es útil para analizar qué funcionó y qué falló después de un incidente de seguridad.

2.2. Evaluación de Riesgos

La gestión de riesgos cibernéticos es el proceso de identificar, priorizar, gestionar y monitorear los riesgos que afectan a los sistemas de información. Es esencial para las empresas debido a su creciente dependencia de la tecnología, lo que las expone a diversas amenazas como ciberataques y errores humanos.

Dado este panorama, entidades como el Instituto Nacional de Estándares y Tecnología (NIST) recomiendan que la gestión de riesgos sea un proceso continuo y no un evento aislado. Revisitar este proceso de forma regular permite a las empresas ajustar sus estrategias a nuevos riesgos y amenazas.

El proceso involucra a ejecutivos (CEO, CISO), equipos de TI y seguridad, legales y otras áreas clave. Las empresas suelen aplicar metodologías como el NIST CSF o el NIST RMF, que siguen pasos similares para gestionar el riesgo.

Metodología de Gestión de Riesgos

1. Enmarcado de riesgos: Definir el contexto de los riesgos permite alinear la gestión de riesgos con la estrategia de negocio. Se consideran aspectos como el alcance, activos críticos, recursos, prioridades y requisitos legales.

2. Evaluación de riesgos: Las empresas identifican amenazas, vulnerabilidades e impactos para crear un perfil de riesgo. Se evalúan las probabilidades y los posibles daños de cada riesgo para priorizar los más críticos.

3. Respuesta al riesgo: Las empresas deciden cómo gestionar los riesgos según su impacto y probabilidad. Las respuestas incluyen mitigar, corregir, aceptar o transferir riesgos.

4. Monitoreo continuo: Se supervisan los controles de seguridad y el panorama de amenazas para ajustar la estrategia en función de cambios en el entorno o la tecnología.

2.3. Cumplimiento Normativo

El cumplimiento normativo en ciberseguridad se refiere a adherirse a las leyes, regulaciones y estándares específicos que rigen la protección de la información en distintos sectores e industrias. La no conformidad puede llevar a sanciones legales, pérdidas financieras y daños reputacionales.

Normativas y Estándares:

GDPR: El Reglamento General de Protección de Datos es una normativa europea que regula la protección de datos personales de ciudadanos de la UE, exigiendo medidas de seguridad, consentimiento del titular y notificación de violaciones.

PCI DSS: Estándar global para proteger datos de tarjetas de pago, que requiere cifrado, controles de acceso y auditorías en organizaciones que manejan transacciones con tarjetas.

ISO 27001: Certificación internacional que establece requisitos para un Sistema de Gestión de Seguridad de la Información, enfocándose en la gestión de riesgos y el compromiso con la protección de la información.

Para asegurar la conformidad con estas normativas, las organizaciones deben implementar controles efectivos.

Estos controles incluyen la creación de políticas y procedimientos sólidos, como políticas de privacidad, controles de seguridad técnica y auditorías internas y externas.
La implementación de encriptación, autenticación multifactor y la segmentación de red, son ejemplos de controles de seguridad técnica esenciales para mitigar riesgos. Las auditorías, tanto internas como externas, permiten evaluar el nivel de cumplimiento y detectar posibles brechas, facilitando la mejora continua.

La gestión de incidentes de cumplimiento es otra parte crucial, ya que prepara a la organización para responder ante violaciones normativas.

Esto implica notificar a las autoridades reguladoras y a los afectados dentro del plazo establecido por la ley, así como investigar los incidentes para identificar su causa y tomar las medidas correctivas necesarias para prevenir futuros incumplimientos.

2.4. Respuesta ante Incidentes

La respuesta a incidentes es un conjunto de procesos y procedimientos diseñados para que las organizaciones puedan prepararse, detectar, contener y recuperarse de incidentes de ciberseguridad, minimizando su impacto en las operaciones y reduciendo los costos asociados.

+ PREPARACIÓN

Es esencial contar con un Plan de Respuesta a Incidentes (IRP), que debe incluir:

Definición de roles y responsabilidades: Identificar quién será responsable en cada fase de la gestión del incidente.
Establecimiento de un equipo de respuesta: Formar un equipo especializado que incluya personal de TI, seguridad, comunicaciones y legal.
Simulacros y entrenamiento: Realizar ejercicios periódicos para probar la eficacia del plan y mejorar la coordinación entre los equipos.

+ DETECCIÓN E IDENTIFICACIÓN

Para una detección efectiva, las organizaciones deben implementar herramientas y procesos que permitan identificar incidentes de seguridad de manera oportuna:

Sistemas de detección: Herramientas que monitorean la red en busca de comportamientos anómalos.
Análisis de logs: Revisión constante de los registros de actividad en busca de indicios de posibles incidentes.

+ CONTENCIÓN Y MITIGACIÓN

Cuando se detecta un incidente, es crucial tomar medidas inmediatas para minimizar su impacto:

Eliminar Malware: Asegurarse de que todo el software malicioso haya sido completamente removido.
Restauración de copias de seguridad: Recuperar los datos y sistemas utilizando respaldos limpios y verificados.

+ ERRADICACIÓN Y RECUPERACIÓN

Tras contener el incidente, es fundamental erradicar la amenaza y restaurar los sistemas a su estado normal:

Aislamiento de sistemas afectados: Desconectar los sistemas comprometidos de la red para evitar la propagación del ataque.
Implementación de parches: Aplicar actualizaciones que eliminen las vulnerabilidades explotadas.

+ ANÁLISIS POST-INCIDENTE

Una vez que el incidente ha sido controlado, se debe realizar una evaluación para extraer lecciones aprendidas y mejorar la preparación para el futuro:

Revisión del incidente: Analizar lo sucedido y cómo se manejó para identificar oportunidades de mejora.
Actualización del IRP: Modificar el plan con base en los aprendizajes obtenidos.

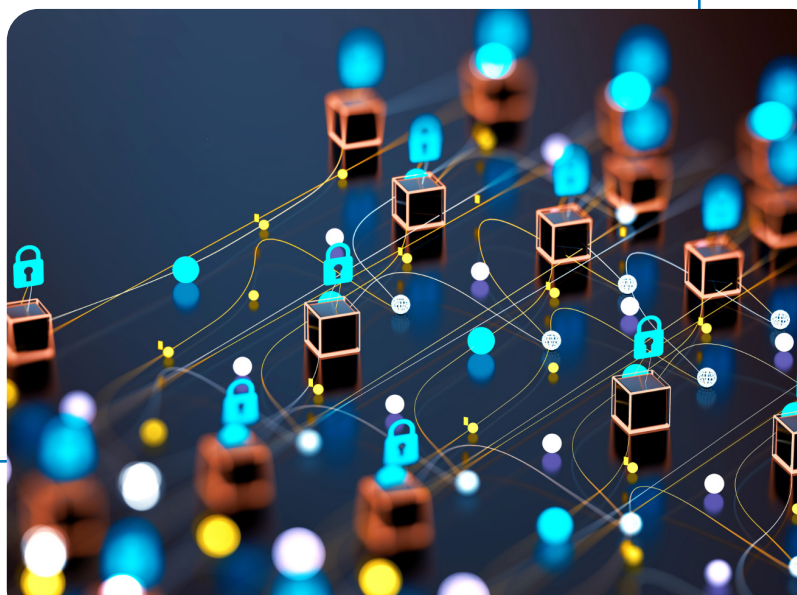
Tipos de Incidentes de Seguridad

Los incidentes de seguridad pueden amenazar la confidencialidad, integridad o disponibilidad de los sistemas de información. Algunos de los más comunes son:

Ransomware: Malware que bloquea los datos o dispositivos, exigiendo un rescate para su liberación.
Phishing: Ataques que engañan a las personas para que compartan información confidencial o ejecuten acciones perjudiciales.
Ataques DDoS: Sobrecargan los recursos de una organización con tráfico masivo, causando interrupciones.
Ataques a la cadena de suministro: Se infiltran en una organización atacando a sus proveedores.
Amenazas internas: Colaboradores o usuarios autorizados que, intencionalmente o por negligencia, comprometen la seguridad de la organización.

Recuerda que este proceso continuo asegura que las organizaciones estén mejor preparadas para enfrentar y mitigar los efectos de ciberataques, minimizando así los riesgos operacionales y financieros.

Mantente siempre un paso adelante de las ciberamenazas



3
Mejores Prácticas de Ciberseguridad

En este capítulo exploramos las mejores prácticas que los líderes deben implementar para fortalecer su infraestructura de seguridad y proteger los activos críticos de la organización. Desde el enfoque Zero Trust hasta la importancia de la cultura de seguridad y la gestión del riesgo, estas prácticas son fundamentales para establecer una postura sólida frente a las amenazas cibernéticas.

3.1. Adopción de una estrategia Zero Trust

Este modelo se basa en la premisa de que no se debe confiar en nadie, tanto dentro como fuera de la red de la organización, y que todos los accesos deben ser verificados y autenticados continuamente. Para los niveles directivos, la adopción de Zero Trust implica un cambio de mentalidad, donde la seguridad ya no se basa en la mera protección perimetral, sino en la defensa constante y en la segmentación de datos, aplicaciones y usuarios. Este enfoque ayuda a prevenir accesos no autorizados y a minimizar los daños en caso de que ocurra una violación de seguridad.

PUNTOS CLAVE

+ **Autenticación multifactor:** Implementar MFA en todos los accesos para reducir riesgos.
+ **Segmentación de redes:** Limitar el acceso a recursos específicos según el rol del usuario.
+ **Visibilidad total:** Es necesario monitorear continuamente todas las actividades dentro de la red.
+ **Control de acceso granular:** Definir políticas estrictas de quién puede acceder a qué información.
+ **Adaptabilidad:** La estrategia debe evolucionar a medida que cambian las amenazas y las infraestructuras.

PREMISA ZERO TRUST

„Nunca confíes, siempre verifica“

3.2. Cultura de Seguridad

Crear una cultura de seguridad implica educar y capacitar a todos los colaboradores, desde el nivel operativo hasta la alta dirección, sobre los riesgos cibernéticos y las mejores prácticas para mitigarlos.

Los líderes deben asegurarse de que la ciberseguridad sea una prioridad compartida, promoviendo políticas claras y fomentando el cumplimiento de protocolos de seguridad. La cultura de seguridad también abarca la responsabilidad de cada individuo para proteger los activos digitales y garantizar que las medidas de seguridad se sigan al pie de la letra.

PUNTOS CLAVE

+ **Compromiso desde la dirección:** Los directivos deben dar ejemplo y priorizar la ciberseguridad.
+ **Capacitación continua:** Educar a todos los colaboradores sobre phishing, ingeniería social y buenas prácticas de seguridad.
+ **Responsabilidad compartida:** Todos los departamentos deben estar alineados en el cumplimiento de las políticas de seguridad.
+ **Políticas claras:** Establecer y comunicar políticas de seguridad comprensibles y prácticas.
+ **Incentivar la denuncia:** Crear un entorno donde los colaboradores se sientan cómodos reportando posibles vulnerabilidades o incidentes.
+ **Conciencia del riesgo:** Los colaboradores deben comprender que sus acciones pueden afectar la seguridad de toda la organización.

3.3. Gestión del Riesgo

Implica identificar, evaluar y priorizar los riesgos cibernéticos a los que una organización está expuesta. Para los líderes, es esencial adoptar un enfoque basado en datos que permita monitorear de manera continua las amenazas y las vulnerabilidades.

Evaluar el riesgo y priorizar inversiones en seguridad son decisiones estratégicas que garantizan la resiliencia de la organización frente a ciberataques.

PUNTOS CLAVE

+ **Automatización:** Implementar tecnologías como inteligencia artificial y aprendizaje automático para detectar amenazas de forma rápida y eficaz.
+ **Sistemas avanzados:** Adoptar tecnologías de detección y respuesta a nivel de endpoints.
+ **Cloud security:** Si la organización usa servicios en la nube, garantizar que las plataformas estén adecuadamente protegidas y gestionadas.
+ **Capacitación y certificaciones:** Asegurar que el equipo de seguridad esté formado y certificado en las últimas tecnologías y metodologías de ciberseguridad.
+ **Contratación especializada:** Identificar brechas de habilidades y contratar expertos en áreas críticas como análisis de vulnerabilidades y respuesta a incidentes.
+ **Retención de talento:** Implementar estrategias de retención, como programas de desarrollo profesional y entornos de trabajo flexibles para evitar la rotación de personal.

3.4. Inversión en Tecnología y Talento

Los directivos deben asegurarse de invertir en las herramientas y plataformas adecuadas que permitan una vigilancia proactiva, detección de amenazas y respuestas automatizadas. Además, deben reconocer la importancia de contratar y retener talento especializado en ciberseguridad.

El mercado de profesionales en ciberseguridad es altamente competitivo, y una inversión adecuada en la formación y retención del personal es clave para el éxito a largo plazo de la estrategia de ciberseguridad.

3.5. Pruebas de Penetración

Las pruebas de penetración, o „pentesting“, son esenciales para evaluar la robustez de las defensas de una organización. Estas pruebas permiten simular ataques reales para identificar debilidades en los sistemas, redes y aplicaciones antes de que los cibercriminales las exploten.

Además ofrece una visión clara de las áreas vulnerables y proporciona una hoja de ruta para mejorar continuamente la postura de seguridad de la organización.

4
Estrategias y Recomendaciones

Este capítulo examina las formas en que las organizaciones pueden integrar la ciberseguridad en sus planes estratégicos, cómo convertirla en una ventaja competitiva y la importancia de colaborar con socios en el ecosistema de seguridad. Además, se profundiza en soluciones proactivas y preventivas clave para mitigar riesgos, adelantarse a amenazas y proteger el futuro de la empresa.

4.1. Integración de la Ciberseguridad en la Estrategia Corporativa

Para los ejecutivos de nivel C, es crucial entender cómo las decisiones estratégicas, como fusiones, adquisiciones o la adopción de nuevas tecnologías, pueden tener implicaciones en la seguridad.

PUNTOS CLAVE

+ **Visión a largo plazo:** La ciberseguridad debe ser parte integral de los objetivos a largo plazo, no solo una medida de emergencia o correctiva.
+ **Adaptación a nuevas tecnologías:** La integración de nuevas tecnologías como tecnologías de engaño o iA.
+ **Políticas de seguridad por área de negocio:** Diferentes áreas requieren diferentes enfoques de seguridad.
+ **Liderazgo:** El liderazgo en ciberseguridad debe comenzar desde el nivel más alto, con la implicación activa de los ejecutivos en la creación de una cultura de seguridad.
+ **Gestión de riesgos estratégicos:** Toda decisión estratégica debe tener en cuenta su impacto en la superficie de ataque de la empresa y en las amenazas potenciales que podrían llegar a surgir.

BENEFICIOS

- Alineación de los objetivos de ciberseguridad con el crecimiento empresarial.
- Reducción de la exposición a riesgos relacionados con nuevos modelos de negocio.
- Mejora en la eficiencia operativa mediante un enfoque proactivo de la seguridad.

4.2. Ciberseguridad como Ventaja Competitiva

Las empresas que priorizan la ciberseguridad no solo mitigan riesgos, sino que también ganan la confianza de sus clientes y socios. Implementar medidas de seguridad avanzadas y demostrar un enfoque proactivo puede diferenciar a la empresa de sus competidores.

PUNTOS CLAVE

+ **Confianza del cliente:** Los clientes valoran las empresas que se toman en serio la seguridad de sus datos. Un enfoque sólido en ciberseguridad mejora la reputación y fideliza a los clientes.
+ **Compliance como diferenciador:** Cumplir con normativas no solo reduce riesgos legales, sino que posiciona a la empresa como un líder en protección de datos.
+ **Protección de la propiedad intelectual (PI):** Proteger las innovaciones y el know-how de la empresa otorga una ventaja competitiva, especialmente en industrias altamente tecnológicas.
+ **Mitigación de interrupciones operativas:** Reducir el tiempo de inactividad debido a incidentes de seguridad garantiza continuidad operativa y minimiza pérdidas económicas.

TÉCNICAS

- **Transparencia y comunicación:** Informar proactivamente a los clientes y socios sobre las medidas de ciberseguridad implementadas.
- **Certificaciones y auditorías:** Obtener certificaciones reconocidas que respalden las capacidades de seguridad de la empresa.
- **Marketing de seguridad:** Posicionar la seguridad como un pilar de la propuesta de valor de la empresa puede atraer a clientes más exigentes y conscientes de los riesgos cibernéticos.

4.3. Colaboración con Especialistas en Ciberseguridad

Ninguna empresa puede enfrentar sola las crecientes amenazas cibernéticas. Colaborar con especialistas en soluciones de ciberseguridad como **LoyalShield** permiten acceder a tecnología avanzada, conocimientos técnicos y capacidades de respuesta ante incidentes, asegurando una defensa más sólida y adaptable.

PUNTOS CLAVE

+ **Integración de nuevas soluciones interempresariales:** Trabajar con socios en la cadena de suministro para asegurar que los estándares de seguridad sean consistentes en todas las etapas.
+ **Participación en foros y eventos de seguridad:** La participación en conferencias, eventos de seguridad como ferias, expos o webinars y capacitaciones facilitan la actualización constante sobre las últimas tendencias en ciberseguridad.

VENTAJAS

- Acceso a inteligencia avanzada sobre amenazas.
- Reducción del tiempo de respuesta ante incidentes.
- Mayor capacidad para cumplir con normativas internacionales de ciberseguridad.

4.4. Soluciones Proactivas y Preventivas

Adoptar soluciones avanzadas es clave para anticiparse a las amenazas y reducir los riesgos, por ello, en **LoyalShield** redefinimos la ciberseguridad para potenciar el éxito de tu negocio. Apostamos por la innovación disruptiva para proteger los activos más valiosos de tus clientes y brindarte la tranquilidad que necesitas.

Deceptive Bytes
Prevention by Deception

Solución basada en engaño para Endpoint

Responde a los ataques que emplean técnicas de evasión, usando una tecnología de simulación única y patentada, colocándola como la solución ideal para proteger e interrumpir los intentos de los atacantes de identificar y comprometer la infraestructura empresarial.

Características principales

Deception Layering: Capas múltiples de engaño para desviar y confundir a los atacantes.
Compatibilidad Amplia: Funciona con varias plataformas y dispositivos.
Automatización Inteligente: Minimiza la intervención humana al ajustar dinámicamente las respuestas de seguridad.

Ventajas

+ Va más allá de la defensa pasiva ya que responde activamente a las amenazas en lugar de solo detectarlas.
+ Al prevenir ataques exitosos, reduce significativamente los costos relacionados con la respuesta y la remediación de incidentes.
+ Disminuye las oportunidades que los cibercriminales tienen para explotar vulnerabilidades.

TWILIGHT CYBER
ONE STEP AHEAD

Protección en tiempo real para tu identidad digital
Detecta si las credenciales de tus clientes han sido comprometidas en la Dark web en horas, a diferencia de otras tecnologías que lo hacen entre 4 y 8 semanas.

Características principales

Previene el Ransomware: Detecta vulnerabilidades y credenciales expuestas en tiempo real, permitiéndote tomar medidas preventivas antes de que los atacantes puedan explotarlas.
Prevención de toma de control de cuentas: Protección de los inicios de sesión de los clientes contra la toma de control de cuentas externas, previniendo el robo de identidad.
Respuesta Rápida a Amenazas: Detección de fugas en 24 horas e información completa de máquinas filtradas y de datos forenses.

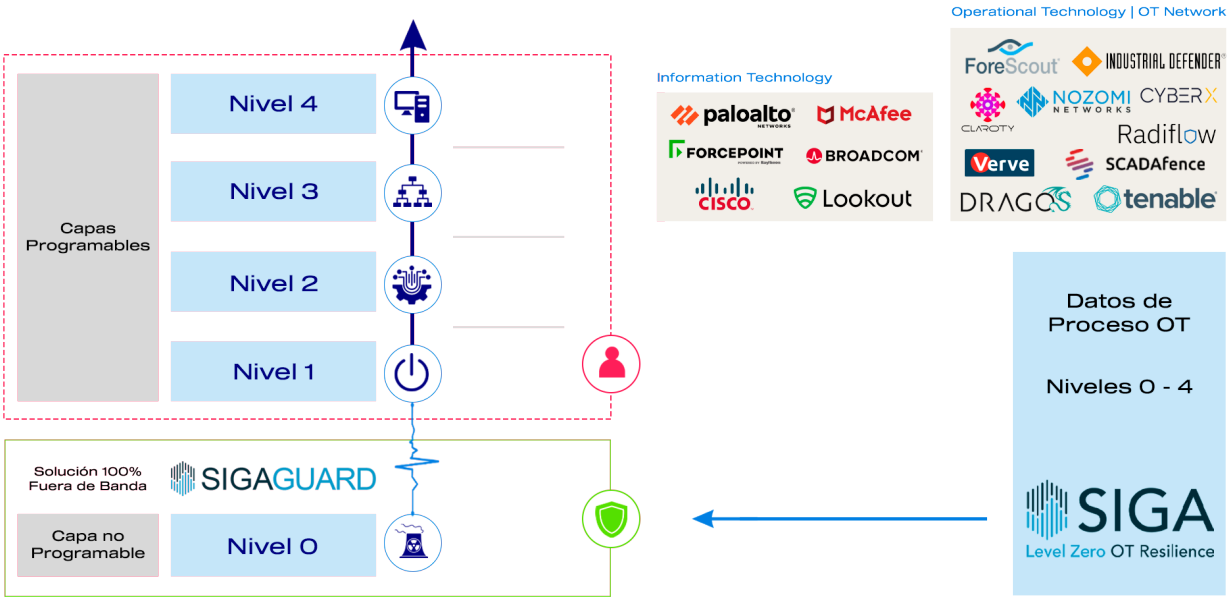
Ventajas

+ Permite actuar en tiempo récord, detectando amenazas dentro de las primeras horas.
+ Nuestra solución asegura la rápida notificación de brechas, permitiéndote actuar con rapidez para neutralizar credenciales comprometidas y contener incidentes.
+ Garantiza la continuidad de tu negocio y la reputación de tu marca al detener los ataques antes de que sucedan.

SIGA Level Zero OT Resilience

Protege los procesos críticos desde capa cero

Protege los activos industriales mediante la monitorización directa de señales eléctricas crudas (realizando un monitoreo en tiempo real desde capa 0), en lugar de depender de los paquetes de datos que pueden ser hackeados.



Características principales

Autónomo: Solución Plug & Play que permite el monitoreo remoto totalmente independiente de la plataforma de ICS.
Confiable: Visión completa y segura de sus operaciones al monitorear las señales eléctricas en la capa física (Nivel 0)
Inteligente: Los algoritmos de aprendizaje automático e IA detectan anomalías cibernéticas que proporcionan información útil para la toma de decisiones.

Ventajas

+ Notifica ciberataques al iniciarse, permitiendo una respuesta rápida y eficiente.
+ Permite monitorear tu maquinaria y mejorar su integridad y continuidad.
+ Monitorea tus activos 24/7, ofreciendo una visualización avanzada las 24 horas del día.
+ Instalación sin interrupciones, obtendrás información invaluable desde el primer día.
+ Trabaja con datos históricos y aprende el modo de operación.

appdome

Protección para aplicaciones móviles
Plataforma integral que proporciona un conjunto de herramientas para automatizar la protección de tus aplicaciones Android e iOS.

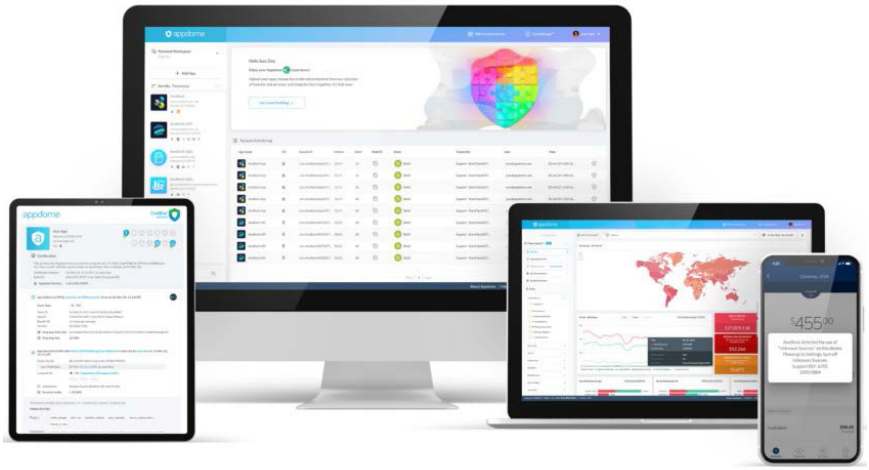
Proporciona 300+ controles de seguridad móvil (medidas antifraude, antimalware, cumplimiento geográfico, etc.) dentro del flujo de trabajo de DevOps móvil.

Características principales

Defensa: Plataforma automatizada diseñada para desarrollar, probar, desplegar y monitorear protecciones en apps Android e iOS en entornos CI/CD.
Cumplimiento: Garantiza la seguridad en tus apps móviles con facilidad. Aplica y controla las defensas, rastrea y reporta el cumplimiento en todo momento.
Control: ThreatScope™; Defensas automáticas desde el primer día para mantener seguras las apps móviles contra ciberataques, fraude y malware en tiempo real.

Ventajas

+ Optimiza la defensa de aplicaciones móviles a nivel empresarial.
+ Integra y cumple fácilmente en tus pipelines de CI/CD utilizando Appdome.
+ Monitorea ataques y defensas en tiempo real y permite respuestas automáticas ante nuevas amenazas.



Al implementar este tipo de soluciones, las empresas no solo reaccionan a los incidentes, sino que se adelantan a ellos, creando un entorno de seguridad robusto y dinámico.