Ciberseguridad y gestión del riesgo organizacional

Breve descripción:

Para abordar la ciberseguridad, se deben comprender sus fundamentos, importancia en el entorno empresarial, normativas y marcos legales relacionados. La ciberseguridad organizacional es un pilar fundamental en la protección de los activos digitales de las empresas, garantizando la continuidad del negocio y la confianza de clientes y socios. Su importancia ha crecido exponencialmente ante la sofisticación de las amenazas cibernéticas en el entorno empresarial moderno.

Agosto de 2025

Tabla de contenido

Introducción

Este componente aborda los conceptos y evolución de la ciberseguridad, resaltando sus características, importancia empresarial y el marco legal aplicable. Se analiza el cibercrimen, sus orígenes y actores, las diferentes formas de delitos informáticos y su impacto tanto local como globalmente. Además, se explora el entorno tecnológico en las organizaciones, detallando componentes, roles y nuevas tendencias digitales. Finalmente, se explica cómo gestionar incidentes de ciberseguridad mediante estándares, políticas organizacionales y el papel clave del Centro de Operaciones de Seguridad (SOC) en la protección continua de la información.

Para comprender la importancia del contenido y los temas abordados, se recomienda acceder al siguiente video:

Video 1. Ciberseguridad y gestión del riesgo organizacional

[Enlace de reproducción del video]

Video 1. Síntesis del video: Ciberseguridad y gestión del riesgo organizacional
En un mundo cada vez más digitalizado, proteger la información se ha convertido en una prioridad para las organizaciones. Este componente formativo explora los fundamentos de la ciberseguridad organizacional, desde su concepto y evolución histórica hasta sus principales características y su papel clave en el entorno empresarial. Asimismo, se abordan las normas y marcos legales que regulan la seguridad de la información a nivel global. La amenaza no es solo técnica, también es humana. Por eso, se examina el fenómeno del cibercrimen, su origen, los actores que lo impulsan y las tipologías de delitos informáticos que afectan tanto a individuos como a grandes corporaciones. Se presenta un panorama nacional e internacional que permite comprender la magnitud de estos riesgos. En este recorrido, también se analiza el entorno de las tecnologías de la información en las organizaciones, reconociendo los servicios, roles y estructuras que permiten operar de manera segura y eficiente. Finalmente, se estudia la gestión de incidentes de ciberseguridad, desde los estándares internacionales hasta las políticas internas y el papel estratégico que desempeñan los Centros de Operaciones de Seguridad, conocidos como SOC. Con este conocimiento, se busca fortalecer la capacidad de respuesta ante amenazas digitales, promoviendo una cultura organizacional orientada a la protección, la prevención y la resiliencia frente a los desafíos del ciberespacio.

1. Ciberseguridad organizacional

La ciberseguridad organizacional es el conjunto de medidas y estrategias que utilizan las empresas para proteger sus computadoras, sistemas, redes e información importante, frente a personas malintencionadas que intentan robar o dañar esos datos. Estas medidas van desde el uso de programas especiales de seguridad, hasta reglas que todos los empleados deben seguir para evitar errores que puedan poner en riesgo la información. Por ejemplo, una empresa puede instalar antivirus, bloquear accesos sospechosos a sus redes y capacitar a sus trabajadores para que no abran correos peligrosos. Todo esto ayuda a mantener la información segura, funcionando correctamente y disponible cuando se necesita. En un mundo cada vez más digital, donde las empresas manejan datos personales, contraseñas, cuentas bancarias y otros datos sensibles por internet, es muy importante protegerlos para evitar consecuencias graves como robos, pérdida de dinero o daños a la reputación de la empresa.

Además de usar herramientas tecnológicas, la ciberseguridad organizacional requiere que las empresas tengan personas capacitadas que identifiquen posibles riesgos y que tomen decisiones para mejorar la protección. También deben cumplir con leyes específicas que exigen cuidar los datos personales de los clientes y reportar si ocurre algún problema de seguridad. No se trata solo de proteger computadoras, sino de enseñar a todos los trabajadores cómo actuar de forma segura. Por ejemplo, usando contraseñas fuertes o no compartiendo información confidencial. Con esto, las empresas pueden seguir funcionando sin interrupciones y los clientes pueden confiar en que su información está protegida.

1.1 Concepto de ciberseguridad

La ciberseguridad es una disciplina esencial en el mundo digital, encargada de proteger sistemas informáticos, redes, dispositivos y datos frente a amenazas cibernéticas y ataques maliciosos. A medida que la tecnología avanza y la interconectividad aumenta, se ha vuelto fundamental para garantizar la privacidad, integridad y disponibilidad de la información en línea.

Se compone de un conjunto de prácticas, tecnologías y procesos diseñados para prevenir accesos no autorizados, daños o pérdidas de datos. Su objetivo principal es garantizar la confidencialidad, integridad y disponibilidad de la información, protegiendo tanto a individuos como a organizaciones de amenazas como virus, malware, ransomware, ataques de denegación de servicio (DDoS) y fraudes digitales.

En un mundo altamente interconectado, un solo ataque cibernético puede generar consecuencias devastadoras, desde el robo de identidad hasta la interrupción de infraestructuras críticas como redes de energía y sistemas de comunicación gubernamentales. Por ello, no solo es crucial para empresas y gobiernos, sino también para los ciudadanos, ya que cada vez más actividades diarias dependen de internet y los sistemas digitales.

A medida que surgen nuevas tecnologías como la Inteligencia Artificial (IA) y el Internet de las Cosas (IoT), los ciberdelincuentes desarrollan métodos de ataque más sofisticados, aprovechando la creciente cantidad de dispositivos conectados. Por este motivo, la protección del ecosistema digital requiere un enfoque integral que combine herramientas avanzadas, normativas adecuadas y una sólida cultura de seguridad.

Para garantizar una protección eficaz, se emplean diversas herramientas y estrategias, como:

- **Firewalls y antivirus**

  Para detectar y bloquear amenazas.
- **Encriptación de datos**

  Para proteger la información sensible.
- **Autenticación multifactor (MFA)**

  Para reforzar el acceso seguro.
- **Monitoreo continuo de redes**

  Para identificar posibles vulnerabilidades.
- Capacitación en seguridad digital para reducir el riesgo de errores humanos.

Uno de los mayores desafíos en ciberseguridad es la falta de concienciación de los usuarios. Muchas brechas de seguridad ocurren debido a prácticas inseguras, como el uso de contraseñas débiles o la apertura de enlaces sospechosos. Por ello, es fundamental fomentar la educación en seguridad digital a nivel individual y organizacional.

La ciberseguridad es un pilar fundamental en la era digital y su relevancia seguirá en aumento. Proteger los datos y las infraestructuras tecnológicas requiere la combinación de tecnologías avanzadas, buenas prácticas organizativas y conciencia individual.

A medida que los ataques evolucionan, también deben hacerlo las estrategias de defensa, asegurando así un entorno digital más seguro y confiable para todos.

1.1 Historia y evolución de la ciberseguridad

La evolución de la ciberseguridad está directamente vinculada al desarrollo de la informática y la expansión de internet. A medida que las tecnologías digitales han avanzado, también lo han hecho las amenazas cibernéticas, lo que ha llevado a la creación de nuevas estrategias y herramientas para proteger la información y las infraestructuras digitales. Desde los primeros sistemas cerrados, hasta el mundo hiperconectado de hoy, la ciberseguridad ha pasado de ser una preocupación limitada a un ámbito técnico a convertirse en una prioridad global para gobiernos, empresas y ciudadanos.

A continuación, se presentan los eventos más relevantes de cada década:

- **Década de 1960-1970 - Los inicios de la ciberseguridad**
  Durante estas décadas, las computadoras eran utilizadas principalmente en entornos cerrados, como universidades y organismos gubernamentales. La seguridad informática se limitaba a la protección del acceso físico a los mainframes, ya que la conectividad era prácticamente inexistente. Sin embargo, con la creación de redes experimentales como ARPANET, surgieron las primeras preocupaciones sobre la seguridad de la información.
- **Década de 1980 - Profesionalización de la ciberseguridad**
  Con la proliferación de computadoras personales y redes más amplias, la seguridad digital comenzó a ganar relevancia. En 1983, el término "ciberseguridad" comenzó a utilizarse para referirse a la protección de sistemas de información. En 1988, el gusano Morris infectó miles de computadoras a través de ARPANET, marcando el primer gran ataque

cibernético de la historia. Este evento impulsó la creación de herramientas como firewalls y software antivirus, así como la fundación de organismos especializados, como el National Computer Security Center (NCSC) en Estados Unidos.

- **Década de 1990 - Auge de internet y nuevas amenazas**

  Con la masificación de internet, surgieron nuevas amenazas como virus informáticos, malware y phishing. Se implementaron tecnologías como los firewalls comerciales y los protocolos de encriptación de datos, como SSL (Secure Sockets Layer), para proteger las transacciones en línea. Las instituciones financieras y empresas comenzaron a adoptar medidas más estrictas para proteger sus redes, aunque los ataques se hicieron cada vez más frecuentes y sofisticados.

- **Década de 2000 - Expansión del comercio digital y los ciberataques**

  La llegada de las redes sociales, el comercio electrónico y el internet de las Cosas (IoT), amplió las vulnerabilidades cibernéticas. Ataques como el gusano “ILoveYou” (2000) y el Blaster Worm (2003) demostraron la capacidad destructiva del malware. En respuesta, se crearon roles especializados, como el Chief Information Security Officer (CISO) y se desarrollaron normativas como la ISO 27001 para estandarizar la seguridad de la información.

- **Década de 2010 - Ciberseguridad como prioridad global**

  La digitalización masiva y la interconectividad expusieron infraestructuras críticas, como redes eléctricas y sistemas de telecomunicaciones, a nuevos riesgos. Los ataques de denegación de servicio (DDoS) y el auge del ransomware pusieron en jaque a empresas y gobiernos. Además,

surgieron las amenazas avanzadas persistentes (APT), impulsadas por grupos organizados y actores estatales. En respuesta, la ciberseguridad comenzó a integrar inteligencia artificial y big data para detectar y mitigar amenazas en tiempo real.

- **Década de 2020 - Nuevos desafíos en un mundo interconectado**
  La pandemia de COVID-19 aceleró el teletrabajo y, con ello, las vulnerabilidades digitales. Los ataques de phishing, ransomware y filtraciones de datos aumentaron significativamente. Las organizaciones incrementaron sus inversiones en ciberseguridad y adoptaron políticas de ciberresiliencia. Actualmente, la seguridad digital enfrenta retos asociados a la inteligencia artificial, la computación cuántica, blockchain y el crecimiento del IoT, lo que ha llevado a los gobiernos a reforzar la regulación y la defensa cibernética a nivel mundial.

A lo largo de estas décadas, la ciberseguridad ha evolucionado en respuesta a la creciente interconexión de sistemas y al aumento de las amenazas cibernéticas. Lo que comenzó como una preocupación limitada a redes cerradas y sistemas gubernamentales, hoy en día afecta a todos los niveles de la sociedad, desde individuos hasta grandes corporaciones y gobiernos. A medida que las tecnologías avanzan, también lo hacen las tácticas de los ciberatacantes, lo que hace que la ciberseguridad siga siendo un desafío constante y de vital importancia.

La historia de la ciberseguridad refleja una batalla continua por proteger la información, la privacidad y la infraestructura crítica, una batalla que continuará a medida que el ciberespacio siga evolucionando.

1.3 Características clave de la ciberseguridad

La ciberseguridad abarca una serie de principios y características fundamentales que buscan proteger la integridad, confidencialidad y disponibilidad de la información. Todas ellas, desempeñan un papel crucial en el diseño y la implementación de sistemas seguros.

A continuación, se explica cada una de estas características principales de la ciberseguridad:

- **Integridad**

  Asegura que la información no sea alterada de manera no autorizada. Esto implica que los datos sean precisos y completos, sin modificaciones maliciosas o accidentales. Se emplean mecanismos como las firmas digitales o códigos hash para verificar que los datos no hayan sido alterados. Por ejemplo, si un archivo es enviado a través de internet, su integridad se puede verificar mediante un código hash, lo que permite comprobar si el archivo ha sido modificado durante el tránsito.

- **Confidencialidad**

  Este principio garantiza que solo las personas o entidades autorizadas puedan acceder a la información. La confidencialidad es crucial para proteger datos sensibles, como información personal, financiera o corporativa. Por ejemplo, se utilizan técnicas como la encriptación de datos para asegurar que incluso si la información es interceptada, no pueda ser leída sin la clave adecuada. Esta característica protege tanto a individuos

como a organizaciones de accesos no autorizados que puedan comprometer su seguridad.

- **Disponibilidad**

  Garantiza que los sistemas y datos sean accesibles cuando los usuarios autorizados los necesiten. Este principio es clave para asegurar que los servicios digitales estén siempre operativos, incluso frente a ataques. La protección contra ataques de denegación de servicio (DoS) o ataques DDoS es un ejemplo claro, ya que estos ataques buscan interrumpir la disponibilidad de un servicio online al sobrecargarlo con tráfico malicioso. Mediante la implementación de infraestructuras de respaldo y sistemas de redundancia, las organizaciones pueden mantener la disponibilidad de sus servicios, incluso en situaciones críticas.

También existen otras características esenciales que complementan y refuerzan la seguridad digital. Estas incluyen:

1. **Autenticidad**

   Garantiza que los usuarios, sistemas y dispositivos sean quienes dicen ser. En un entorno digital, la autenticidad es esencial para evitar fraudes y suplantaciones de identidad. Se asegura mediante métodos como autenticación multifactor (MFA), que exige más de un factor (contraseña, huella dactilar, código enviado a un teléfono, etc.) para verificar la identidad del usuario, antes de permitir el acceso a un sistema.

2. **No repudio**

   Asegura que una vez que una transacción o acción es realizada, no pueda ser negada por la persona o entidad que la efectuó. Este principio es crucial para mantener la responsabilidad y la trazabilidad en las interacciones digitales. Los registros de auditoría y las firmas digitales, juegan un papel clave en este aspecto, ya que permiten rastrear las acciones realizadas y verificar que no se pueda negar la ejecución de una acción en un sistema.

3. **Escalabilidad**

   En ciberseguridad, la escalabilidad se refiere a la capacidad de un sistema para adaptarse y proteger una creciente cantidad de datos, usuarios o dispositivos sin comprometer la seguridad. A medida que las empresas y los usuarios aumentan su presencia en línea, las soluciones de ciberseguridad deben ser capaces de ajustarse para cubrir nuevas amenazas y el crecimiento de la infraestructura, sin disminuir la efectividad de la protección.

4. **Resiliencia**

   Se refiere a la capacidad de un sistema para recuperarse rápidamente de un incidente de seguridad. No solo se trata de prevenir ataques, sino también de responder de manera rápida y efectiva ante incidentes. Los planes de recuperación ante desastres, los sistemas de respaldo y las copias de seguridad, son fundamentales para garantizar que, en caso de un

ataque, los sistemas puedan restaurarse lo más rápido posible, sin grandes pérdidas de datos o interrupciones de servicio.

5. **Seguridad proactiva**

   A diferencia de la seguridad reactiva, que responde a incidentes después de que ocurren, la seguridad proactiva implica anticiparse a las amenazas antes de que sucedan. Esto incluye la implementación de monitoreo constante, análisis de vulnerabilidades y el uso de inteligencia de amenazas para identificar patrones y posibles riesgos antes de que los atacantes los exploten.

6. **Cumplimiento normativo**

   La ciberseguridad también implica cumplir con las leyes y regulaciones vigentes que afectan la protección de datos e infraestructura. Esto incluye marcos regulatorios como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea o la Ley de Privacidad del Consumidor de California (CCPA), que requieren que las organizaciones adopten medidas estrictas para proteger los datos personales de los usuarios. Cumplir con estos estándares no solo es una obligación legal, sino también una forma de ganar la confianza de los usuarios.

7. **Transparencia**

   En ciberseguridad, implica que las organizaciones comuniquen de manera clara y abierta las medidas de protección que están implementando, así como los riesgos potenciales. Las auditorías y los informes de seguridad

ayudan a asegurar que las partes interesadas puedan evaluar cómo una organización maneja sus riesgos de seguridad.

Las características de la ciberseguridad no solo cubren la protección básica de la información, sino que también abordan aspectos esenciales como la autenticación, la resiliencia y el cumplimiento normativo, entre otros. La implementación efectiva de estas características es crucial para proteger, tanto a individuos como a organizaciones de las amenazas digitales cada vez más sofisticadas.

A medida que los sistemas digitales se expanden y evolucionan, la seguridad debe adaptarse para enfrentar nuevos desafíos y estas características deben ser la base sobre la cual se construyan las estrategias de ciberseguridad.

1.4 Importancia de la ciberseguridad en el entorno empresarial

La ciberseguridad es muy importante para las empresas, porque ayuda a proteger toda la información que manejan día a día, como datos personales de los clientes, documentos internos, contraseñas y cuentas bancarias. En el mundo actual, la mayoría de las empresas depende de sistemas digitales y del internet para funcionar, lo que las hace vulnerables a diferentes tipos de amenazas, como hackers que intentan robar información, virus que dañan los sistemas o correos falsos que engañan a los empleados. Si ocurre un ataque de este tipo, la empresa puede perder mucho dinero, dejar de funcionar por un tiempo o incluso tener problemas con la ley. Pero aún más grave puede ser que los clientes pierdan la confianza en esa empresa y decidan no seguir comprando o contratando sus servicios. Por eso, la ciberseguridad no solo protege los datos, también ayuda a que la empresa siga funcionando sin interrupciones y mantenga su buena reputación.

Además, tener buena ciberseguridad permite que las empresas usen nuevas tecnologías con mayor seguridad, como el trabajo desde casa, las ventas en línea o el almacenamiento de información en la nube. Para muchas empresas, cumplir con leyes y normas de protección de datos también es obligatorio y no hacerlo puede traerles multas o sanciones. Al cuidar bien sus sistemas, las empresas pueden adelantarse a los problemas, evitar daños grandes y demostrar que son responsables con la información que manejan. Por eso, invertir en ciberseguridad no es un gasto innecesario, sino una forma de asegurar el futuro del negocio.

En resumen, la ciberseguridad es fundamental para que cualquier empresa funcione de forma segura, mantenga la confianza de sus clientes y se adapte a los cambios del mundo digital.

1.5 Normas y marcos legales relacionados

Las normas y regulaciones internacionales en ciberseguridad, establecen marcos de referencia, buenas prácticas y requisitos técnicos que permiten proteger la información en diversos contextos. Estas normativas son esenciales para guiar a organizaciones y gobiernos en la creación de políticas y sistemas de seguridad robustos, ayudando a mitigar los riesgos cibernéticos y garantizar la protección de los datos.

A continuación, se presentan algunas de las más reconocidas:

Tabla 1. Principales normas y regulaciones internacionales en ciberseguridad

Norma/Regulación	Descripción	Objetivo
ISO/IEC 27001.	Estándar internacional para la gestión de la seguridad de la información (SGSI).	Establecer, implementar, mantener y mejorar un sistema de gestión de seguridad.
ISO/IEC 27002.	Guía de controles de seguridad de la información basada en ISO 27001.	Apoyar en la selección de medidas de seguridad adecuadas.
ISO/IEC 27018.	Directrices para la protección de la información personal en la nube.	Proteger la privacidad de los datos personales en los servicios de computación en la nube.
NIST Cybersecurity Framework.	Marco de referencia de ciberseguridad desarrollado por el National Institute of Standards and Technology.	Proporcionar directrices para mejorar la gestión de riesgos de ciberseguridad.
GDPR (Reglamento General de Protección de Datos).	Reglamento europeo que regula la protección de datos personales.	Garantizar los derechos de los usuarios, el consentimiento y el almacenamiento seguro de datos.

Norma/Regulación	Descripción	Objetivo
PCI-DSS (Payment Card Industry Data Security Standard).	Estándar para proteger los datos de tarjetas de pago.	Asegurar la protección de datos sensibles de las tarjetas de crédito/débito.
HIPAA (Health Insurance Portability and Accountability Act).	Estándar de protección de la información de salud personal en EE.UU.	Asegurar la privacidad y la protección de los datos de salud personales.
FISMA (Federal Information Security Management Act).	Norma para proteger los sistemas de información en agencias federales de EE.UU.	Establecer requisitos de seguridad para proteger las infraestructuras críticas del gobierno.
Cybersecurity Act of 2015.	Ley de ciberseguridad de EE.UU. para fomentar la colaboración público-privada.	Mejorar la colaboración para enfrentar amenazas cibernéticas y fomentar el intercambio de información.
SOC 2.	Estándar de auditoría para la seguridad, confidencialidad, integridad, etc.	Asegurar que los servicios en la nube cumplan con los requisitos de seguridad y privacidad.

Norma/Regulación	Descripción	Objetivo
OECD Privacy Guidelines.	Directrices internacionales de la OCDE para la protección de la privacidad.	Establecer estándares globales para la protección de la privacidad y los flujos de datos.

Estas normas no solo ofrecen un enfoque integral para la ciberseguridad, sino que también buscan armonizar las mejores prácticas a nivel mundial, permitiendo la protección de la información en entornos cada vez más globalizados y digitales.

2. Delitos informáticos y cibercrimen

Los delitos informáticos y el cibercrimen, son acciones ilegales que se realizan usando computadoras, teléfonos, internet u otros dispositivos tecnológicos. Estas actividades buscan dañar, robar información o sacar beneficios engañando a personas o afectando sistemas. Algunos ejemplos comunes son el robo de contraseñas, enviar virus a otros equipos, hacer compras con tarjetas robadas por internet o engañar con correos falsos (phishing) para que la gente entregue sus datos personales. También existen ataques que pueden bloquear el funcionamiento de páginas web o sistemas completos, afectando a personas, empresas e incluso gobiernos. Estos delitos se han vuelto más frecuentes porque internet se usa en casi todos los aspectos de la vida diaria de las personas, como estudiar, trabajar, comprar y comunicarse.

Este tipo de delitos puede causar muchos problemas: desde pérdida de dinero hasta la exposición de información privada, como fotos, documentos importantes o datos bancarios. También pueden dañar la imagen de una empresa, si sus clientes pierden la confianza por una filtración. Por eso es muy importante aprender a protegerse usando contraseñas seguras, no compartiendo información con desconocidos y teniendo cuidado con los enlaces o archivos sospechosos.

Las autoridades de muchos países también han creado leyes para castigar a los delincuentes cibernéticos, pero lo más importante es prevenir. Con educación, buenas prácticas y medidas de seguridad, todos pueden ayudar a que internet sea un lugar más seguro para todos.

2.1 Origen y evolución del cibercrimen

A continuación, se detalla la evolución que ha tenido el cibercrimen, en los diferentes procesos tecnológicos que hacen parte de la ciberseguridad:

- **Década de 1950-1970 - Los inicios de los delitos informáticos**

  El origen de los delitos informáticos está ligado al desarrollo temprano de la computación y las primeras redes de comunicación. En los años 50 y 60, las computadoras eran utilizadas principalmente en universidades, gobiernos y empresas. Durante esta época, no existía una infraestructura global como internet, por lo que los delitos informáticos eran limitados. Sin embargo, el concepto de manipulación de sistemas informáticos comenzó a discutirse, sentando las bases para futuras amenazas.

- **Década de 1980 - El auge del malware y el fraude informático**

  Con la llegada de las computadoras personales y la expansión de las redes, surgieron los primeros delitos informáticos claramente definidos. Durante este período, el uso de malware (software malicioso) comenzó a ganar notoriedad, con los primeros virus diseñados para replicarse y dañar computadoras. Un ejemplo temprano fue el virus "Brain" en 1986, considerado uno de los primeros en afectar computadoras a gran escala. Además, se registraron casos de fraude informático y robo de datos, aprovechando las redes para cometer estafas financieras.

- **Década de 1990 - La expansión de internet y los ciberataques**

  Con la proliferación de internet, los delitos informáticos se diversificaron y se convirtieron en una preocupación global. La piratería informática (hacking) comenzó a afectar a gobiernos y empresas, con ataques

dirigidos al robo de información confidencial. También surgieron los delitos cibernéticos financieros, como el phishing y el fraude en línea. En 1994, se reportó uno de los primeros casos importantes de fraude con tarjetas de crédito en línea, marcando un punto de inflexión en la cibercriminalidad.

- **Década de 2000 - Cibercrimen organizado y ransomware**

  A medida que internet se consolidó como una plataforma global de comunicación y comercio, los delitos informáticos se volvieron más organizados. Durante esta década, las organizaciones criminales comenzaron a utilizar la red para llevar a cabo actividades ilegales a gran escala, incluyendo el robo de datos personales y ataques DDoS (Denegación de Servicio Distribuido). Uno de los delitos informáticos más notorios de la época fue el ransomware, un tipo de ataque en el que los delincuentes cifran los archivos de la víctima y exigen un rescate para liberarlos. Ejemplos como el virus "Klez" a principios de los 2000 ilustran este creciente problema.

- **Década de 2010 - Amenazas avanzadas y filtraciones masivas**

  El auge del internet de las Cosas (IoT), la computación en la nube y las redes sociales amplió el alcance de los delitos informáticos. Los ataques de ransomware se volvieron más sofisticados y las filtraciones de datos afectaron a millones de usuarios. Empresas de alto perfil, como Yahoo! y Equifax, sufrieron violaciones de seguridad masivas. Además, los ataques cibernéticos patrocinados por estados y las Amenazas Persistentes Avanzadas (APT) se convirtieron en una preocupación creciente, con hackers infiltrándose en sistemas gubernamentales y empresariales para el espionaje político, económico y militar.

- **Década de 2020 - Ciberataques sofisticados y nuevas tecnologías**

  La actualidad ha sido testigo de un aumento en la sofisticación de los delitos informáticos. Entre los ataques más comunes se encuentran el phishing dirigido, el fraude financiero mediante criptomonedas y los ciberataques a infraestructuras críticas, como hospitales y redes eléctricas. Como se mencionó, la pandemia de COVID-19 impulsó el teletrabajo y, con él, un incremento en los ciberataques, como el ransomware. Además, los cibercriminales están empleando inteligencia artificial y machine learning para hacer sus ataques más complejos y evasivos. Asimismo, los ataques a la cadena de suministro han aumentado, comprometiendo a proveedores de software para infiltrarse en las redes de sus clientes.

Los delitos informáticos han evolucionado desde simples actos de hacking hasta operaciones criminales altamente organizadas que afectan a individuos, empresas y gobiernos en todo el mundo. Con el avance de la tecnología, las amenazas continúan diversificándose, lo que hace imprescindible la adopción de estrategias de ciberseguridad robustas y la colaboración internacional para mitigar estos riesgos.

La innovación en seguridad digital, junto con la concienciación de los usuarios, seguirá siendo clave para enfrentar los desafíos del cibercrimen en el futuro.

2.2 Principales actores involucrados en los delitos informáticos

En el panorama actual de la ciberseguridad, comprender quiénes son los responsables de las amenazas digitales es tan importante como conocer las técnicas que emplean. Los actores del cibercrimen son individuos o grupos que utilizan la tecnología con fines maliciosos, ya sea para obtener beneficios económicos, causar

daño, robar información o interrumpir servicios. Estos actores no son homogéneos, ya que varían en sus motivaciones, nivel de sofisticación, recursos y objetivos.

Desde piratas informáticos solitarios que buscan notoriedad, hasta organizaciones criminales bien estructuradas e incluso actores patrocinados por Estados, el cibercrimen ha evolucionado hacia un ecosistema complejo y dinámico. Identificar y clasificar a estos actores permite a los profesionales de la seguridad anticipar amenazas, diseñar estrategias de defensa efectivas y fortalecer la resiliencia de los sistemas digitales.

A continuación, se describen algunos de los principales actores del cibercrimen:

1. **Black hat hackers**

   Expertos en informática que explotan vulnerabilidades con fines ilícitos, como el robo de datos o la distribución de malware.

2. **Ciberterroristas**

   Utilizan ataques informáticos para causar pánico o daño a entidades gubernamentales o infraestructuras críticas.

3. **Criminales organizados**

   Redes delictivas que operan en la web oscura para cometer fraudes, extorsiones y otros delitos financieros.

4. **Insiders**

   Empleados o exempleados que abusan de su acceso a sistemas internos para sabotaje, robo de información o espionaje corporativo.

5. **Hacktivistas**

   Individuos o grupos que emplean ataques cibernéticos con motivaciones políticas o ideológicas, como la filtración de documentos confidenciales.

6. **Actores patrocinados por Estados**

   Grupos respaldados por gobiernos que realizan ciberespionaje, sabotaje o ataques dirigidos contra otras naciones.

La comprensión de los actores del cibercrimen es fundamental para diseñar estrategias de defensa efectivas y mitigar los riesgos asociados a las amenazas digitales. Cada uno de estos actores opera con motivaciones y metodologías distintas, lo que obliga a las organizaciones y gobiernos a mantenerse en constante actualización para enfrentar nuevos desafíos en seguridad informática.

La cooperación internacional, la educación en ciberseguridad y el desarrollo de tecnologías avanzadas son esenciales para contrarrestar el impacto de estas actividades maliciosas y proteger la integridad de la información en un entorno digital cada vez más complejo.

2.3 Tipologías de actos ilícitos digitales

Los delitos informáticos abarcan una amplia gama de actividades ilícitas que afectan a individuos, empresas y gobiernos. Algunos de los más comunes incluyen:

- **Cibercrimen financiero**

  Fraudes como el robo de tarjetas de crédito, phishing, suplantación de identidad y estafas en línea, con el objetivo de obtener beneficios económicos de manera fraudulenta.

- **Malware**

  Desarrollo y propagación de software malicioso (ransomware, troyanos, virus) para robar información, dañar sistemas o extorsionar a las víctimas mediante el secuestro de datos.

- **Ataques a infraestructuras críticas**

  Ciberataques dirigidos a sistemas esenciales, como redes de energía, transporte, salud y servicios financieros, con el fin de interrumpir su funcionamiento o comprometer su seguridad.

- **Ciberespionaje**

  Robo de información confidencial por parte de actores estatales o grupos organizados, con el propósito de obtener ventajas políticas, económicas o militares a través de la infiltración en sistemas estratégicos.

- **Delitos contra la privacidad**

  Uso indebido de datos personales para extorsión, suplantación de identidad o comercialización ilegal en la web oscura, lo que compromete la seguridad y derechos de las víctimas.

- **Ataques DDoS (Denegación de Servicio Distribuida)**

  Saturación intencional de un sistema con tráfico falso para afectar su disponibilidad, generando interrupciones en plataformas y servicios en línea.

- **Delitos sexuales en línea**

  Actividades ilícitas como la explotación infantil, distribución de material de abuso sexual, el ciberacoso y el grooming, que afectan la integridad y seguridad de las personas en entornos digitales.

Los delitos informáticos continúan evolucionando a medida que la tecnología avanza, lo que representa un desafío constante para las autoridades y los profesionales de la ciberseguridad. La sofisticación de los ataques, junto con la expansión del acceso a internet y el crecimiento del cibercrimen organizado, hace imprescindible la implementación de estrategias de prevención, detección y respuesta efectivas.

La cooperación internacional, el desarrollo de marcos normativos actualizados y la concienciación de los usuarios son clave para mitigar los riesgos y fortalecer la seguridad en el entorno digital.

2.4 Panorama de los delitos informáticos en el contexto nacional e internacional

En Colombia, los delitos informáticos están regulados por la Ley 1273 de 2009, que modificó el Código Penal para incluir sanciones específicas relacionadas con el acceso no autorizado, la alteración de datos y el uso indebido de tecnologías de la información y las comunicaciones. Esta normativa protege la integridad de los sistemas informáticos, la confidencialidad de la información y la privacidad de los usuarios.

Los principales delitos contemplados en la ley incluyen:

1. **Acceso abusivo a sistemas informáticos**

   Ingreso no autorizado a redes, bases de datos o plataformas digitales.

2. **Interceptación de datos informáticos**

   Captura ilegal de información transmitida en redes privadas o públicas.

3. **Uso de software malicioso**

   Creación, propagación o utilización de programas diseñados para causar daño o vulnerar la seguridad digital.

4. **Violación de datos personales**

   Recopilación, modificación o divulgación no autorizada de información privada con fines ilícitos.

5. **Interferencia en sistemas o datos**

   Alteración, eliminación o daño de información almacenada en medios electrónicos.

6. **Fraude informático**

   Manipulación de sistemas informáticos para obtener beneficios económicos de manera ilícita.

La Ley 1273 de 2009 establece penas de prisión y multas, cuya severidad varía según la naturaleza y el impacto del delito cometido. Además, refuerza la responsabilidad de las instituciones y empresas en la protección de datos y la seguridad de la información, promoviendo el desarrollo de estrategias de prevención y respuesta ante amenazas cibernéticas.

Los delitos informáticos son una preocupación global que afecta a individuos, empresas, gobiernos y otras organizaciones en todo el mundo. A medida que la tecnología ha avanzado y el internet se ha convertido en un pilar fundamental de la vida diaria, las amenazas cibernéticas han evolucionado y se han sofisticado. Los delitos informáticos son un fenómeno creciente y no se limitan a un solo país o región, sino

que afectan a nivel global, atravesando fronteras y presentando desafíos tanto para las leyes nacionales como para la cooperación internacional. Los delitos informáticos tienen su origen en las primeras computadoras conectadas en redes. Durante las primeras décadas de la informática, los delitos informáticos eran limitados, principalmente por el acceso no autorizado a sistemas. Sin embargo, a medida que el internet y las redes globales crecieron, los ciberdelincuentes encontraron nuevas formas de atacar sistemas y robar información valiosa, lo que impulsó el desarrollo de legislación específica y organismos especializados en la lucha contra estos delitos.

En las últimas dos décadas, los delitos informáticos han crecido de manera exponencial, impulsados por la expansión del uso de tecnologías como los smartphones, las computadoras portátiles, el Internet de las Cosas (IoT) y el comercio electrónico. Además, retomando lo mencionado previamente, la pandemia de COVID-19 aceleró la digitalización de las actividades cotidianas, lo que resultó en un aumento significativo de los ciberataques, especialmente los de ransomware y el fraude en línea. Los cibercriminales ahora operan en organizaciones criminales estructuradas, con objetivos financieros, políticos y, en algunos casos, militares.

Dentro de las tendencias actuales, uno de los ataques más graves es el ransomware, donde los ciberdelincuentes secuestran los sistemas de las víctimas, cifran sus datos y exigen un pago, generalmente en criptomonedas, para restaurar el acceso. Además, la expansión del teletrabajo durante la pandemia ha abierto nuevas oportunidades para los ciberdelincuentes, con un aumento de los ataques de phishing dirigidos a empleados que utilizan plataformas de colaboración remota.

El cibercrimen patrocinado por el Estado también ha aumentado, con ataques a infraestructuras críticas y elecciones. Un ejemplo claro es el ciberataque a las

elecciones presidenciales de EE. UU. en 2016, donde se acusó a actores rusos de interferir en el proceso electoral. Asimismo, el robo de datos y la privacidad sigue siendo una amenaza persistente, como lo evidenció el ataque a Facebook en 2021, que expuso los datos personales de más de 530 millones de usuarios.

La creciente popularidad de las criptomonedas también ha facilitado actividades ilegales, como el lavado de dinero y el uso de mercados oscuros en la web. Además, el cibercrimen se ha extendido al ámbito de la desinformación, donde los cibercriminales manipulan la opinión pública mediante fake news y bots en redes sociales, afectando elecciones, movilizaciones y creando caos social.

A pesar de los esfuerzos por mejorar la cooperación internacional, la lucha contra los delitos informáticos enfrenta desafíos debido a la falta de un marco legal homogéneo a nivel global y las diferencias en las capacidades tecnológicas entre países. Los ciberdelincuentes, a menudo, explotan estas diferencias y la falta de regulación uniforme, lo que complica aún más la respuesta efectiva frente a estas amenazas.

La lucha contra el cibercrimen enfrenta una serie de retos complejos debido a la naturaleza transnacional de los delitos, las variaciones en las legislaciones de diferentes países y la rápida evolución de las tecnologías utilizadas por los ciberdelincuentes. Estos desafíos requieren una cooperación más efectiva entre países, una actualización constante de las normativas y el uso de tecnologías avanzadas tanto por las autoridades como por los delincuentes.

A continuación, se describen algunos de los principales obstáculos que dificultan la lucha global contra el cibercrimen:

1. **Falta de cooperación internacional**

   Aunque existen acuerdos como la Convención de Budapest (un tratado internacional para combatir la cibercriminalidad), las diferencias en las leyes nacionales y la falta de cooperación efectiva entre países dificultan la persecución de ciberdelincuentes, especialmente cuando estos operan en territorios con legislaciones débiles o inexistentes en cuanto a delitos informáticos.

2. **Desafíos legales y regulatorios**

   Las leyes de ciberseguridad y privacidad aún están en proceso de estandarizarse globalmente. Muchos países no cuentan con legislación específica que aborde todos los aspectos de los delitos informáticos, lo que permite que los ciberdelincuentes exploten brechas legales y operen sin temor a sanciones adecuadas.

3. **Evolución rápida de las amenazas**

   Los ciberdelincuentes son cada vez más sofisticados y utilizan tecnologías avanzadas, como inteligencia artificial y machine learning, para mejorar sus ataques, lo que representa un reto para los gobiernos y las empresas, que deben adaptarse constantemente a nuevas amenazas. Además, la automatización y el uso de herramientas como ransomware-as-a-service han permitido a actores menos especializados lanzar ataques cibernéticos de gran escala.

4. **Falta de recursos en países en desarrollo**

   Muchos países no cuentan con los recursos humanos y tecnológicos necesarios para enfrentar el cibercrimen de manera efectiva. Esto genera una disparidad en la capacidad de los diferentes países para proteger sus

infraestructuras críticas, regular las actividades en línea y perseguir a los responsables de delitos informáticos.

La lucha contra el cibercrimen requiere de un enfoque integral que implique la colaboración internacional, la actualización constante de las normativas y el desarrollo de tecnologías avanzadas para contrarrestar las tácticas, cada vez más sofisticadas de los ciberdelincuentes. Solo mediante la cooperación y el fortalecimiento de las capacidades nacionales e internacionales se podrá enfrentar esta amenaza global de manera efectiva.

El ciberespacio es un entorno digital en constante evolución que ha transformado la interacción global, dando origen a la ciberseguridad como una disciplina clave para proteger la información y los sistemas tecnológicos. A lo largo de su historia, la ciberseguridad ha desarrollado normativas y principios esenciales para mitigar riesgos y enfrentar desafíos como los delitos informáticos, los cuales afectan a individuos, empresas y gobiernos a nivel mundial. Estos delitos, cometidos por diversos actores del cibercrimen, incluyen fraudes electrónicos, robo de datos y ataques a infraestructuras críticas, lo que ha impulsado la creación de regulaciones y estrategias de prevención.

En Colombia y en el mundo, la lucha contra el cibercrimen enfrenta desafíos como la falta de cooperación internacional y la rápida evolución de las amenazas digitales. Para contrarrestar estos riesgos, existen mecanismos de reporte y medidas de prevención que buscan fortalecer la seguridad digital y la protección de la información.

3. Entorno de tecnologías de la información en las organizaciones

El entorno de Tecnologías de la Información (TI) en las organizaciones, es el conjunto de herramientas, sistemas y recursos que permiten manejar y procesar la información de manera digital. Aunque muchos piensan que la tecnología solo se refiere a computadoras, abarca mucho más: incluye redes de comunicación, software especializado, bases de datos, servidores, sistemas en la nube y dispositivos móviles. Todo esto se integra para ayudar a que la organización funcione de manera más eficiente, rápida y segura. Por ejemplo, gracias a las TI, es posible almacenar enormes cantidades de datos de forma ordenada y acceder a ellos cuando se necesiten, lo que facilita la toma de decisiones informadas. Además, permiten la comunicación instantánea mediante correos electrónicos, videollamadas y chats, reduciendo las distancias y agilizando el trabajo en equipo, incluso si los empleados están en diferentes lugares del mundo. La automatización de procesos rutinarios, como la gestión de facturas o la atención al cliente, libera tiempo para que las personas se concentren en tareas más importantes y creativas. También, las TI juegan un papel clave en la seguridad de la información, protegiendo datos confidenciales contra posibles fraudes o ataques. Por otro lado, permiten analizar grandes volúmenes de información, identificando tendencias y oportunidades de mejora que de otra forma serían difíciles de detectar. Para cualquier organización, invertir en tecnologías de la información no solo es imprescindible para sobrevivir, sino también para crecer y diferenciarse en el mercado actual.

3.1 Servicios y roles asociados a la infraestructura tecnológica

A continuación, en un video, se aborda la definición y componentes de las TI, servicios y roles asociados a la infraestructura tecnológica y tendencias emergentes en el entorno digital en la siguiente historia:

Video 2. Análisis forense y profesionalización en ciberseguridad. El descubrimiento ¿Qué son las TIC?

Enlace de reproducción del video

Video 2. Síntesis del video: Análisis forense y profesionalización en ciberseguridad. El descubrimiento ¿Qué son las TIC?

Sofía, una joven emprendedora, decidió iniciar un pequeño negocio. Al poco tiempo, descubrió que casi todo lo que hacía en su día a día dependía de las Tecnologías de la Información (TI). Un asesor le explicó que las TI son el conjunto de herramientas y sistemas que permiten almacenar, procesar y transmitir información de forma digital.

Los componentes: mucho más que computadoras

Mientras organizaba su nuevo negocio, Sofía se dio cuenta de que las TI habían evolucionado mucho. Ya no se trataba solo de computadoras. Descubrió que se componen principalmente de tres elementos:

- **Hardware**

  Dispositivos físicos como computadoras, servidores, impresoras y smartphones.
- **Software**

  Programas y aplicaciones que permiten realizar tareas, desde procesar textos hasta gestionar grandes bases de datos.
- **Redes y conectividad**

  Permiten que los dispositivos y sistemas se comuniquen entre sí, ya sea localmente (red interna) o a través de internet.

Todo esto, integrado, daba forma al entorno tecnológico que haría crecer su emprendimiento.

Los servicios y roles: detrás de cada sistema, gente clave

Sofía observó que, para que todo funcionara correctamente, necesitaba diferentes servicios y especialistas. Aprendió sobre algunos roles esenciales:

- **Administradores de sistemas**

  Garantizan que los servidores y redes funcionen sin problemas.

- **Soporte técnico**

  Ayudan a resolver problemas diarios de computadoras y programas.

- **Desarrolladores de software**

  Crean y adaptan aplicaciones según las necesidades del negocio.

- **Especialistas en ciberseguridad**

  Protegen la información y los sistemas de posibles amenazas.

Además, conoció conceptos como la nube, que permite almacenar archivos y utilizar aplicaciones sin depender de un solo equipo.

Video 3. Análisis forense y profesionalización en ciberseguridad. Tendencias emergentes: el futuro ya llegó

Enlace de reproducción del video

Video 3. Síntesis del video: Análisis forense y profesionalización en ciberseguridad. Tendencias emergentes: el futuro ya llegó
Con curiosidad, Sofía investigó las tendencias emergentes en el entorno digital y se sorprendió al ver cómo la tecnología avanza: • **Inteligencia Artificial (IA)** Sistemas capaces de aprender y tomar decisiones para automatizar procesos y personalizar la experiencia de clientes.

- **Internet de las cosas (IoT)**

  Dispositivos conectados, como sensores, cámaras y electrodomésticos inteligentes, que recopilan y transmiten datos en tiempo real.

- **Computación en la nube**

  Permite trabajar a distancia y acceder a grandes recursos tecnológicos sin invertir en infraestructura costosa.

- **Ciberseguridad avanzada**

  Uso de soluciones basadas en IA y análisis predictivo para proteger los datos.

- **Transformación digital**

  Integración de tecnologías en todos los procesos, haciendo que los negocios sean más ágiles y competitivos.

Un entorno en permanente evolución

A través de este viaje, Sofía comprendió que las TI no solo son el motor de su emprendimiento, sino el corazón de la transformación de las organizaciones modernas. Adaptarse y aprender sobre nuevas tendencias le permitió descubrir oportunidades para crecer y mantenerse competitiva en un mundo cada vez más conectado y digital.

4. Gestión de incidentes de ciberseguridad

La gestión de incidentes de ciberseguridad, consiste en un conjunto de prácticas y procesos diseñados para detectar, responder, mitigar y documentar eventos que ponen en riesgo la información o los sistemas de una organización. Es fundamental porque reduce el impacto de ataques y minimiza la interrupción del negocio.

Antes, las organizaciones reaccionaban a los incidentes de forma aislada y sin planificación; hoy, existen equipos dedicados (como CSIRT o SOC) que usan metodologías probadas y herramientas sofisticadas para la gestión de incidentes.

Ejemplo práctico

Imagine una empresa que detecta acceso no autorizado a su red un sábado por la noche. El equipo responsable sigue estos pasos:

1. **Preparación**: han entrenado previamente a su personal y cuentan con manuales de acción.
2. **Identificación**: monitorean las alertas de su firewall e identifican el acceso sospechoso.
3. **Contención**: aíslan el sistema comprometido para evitar que el ataque se propague.
4. **Erradicación/Mitigación**: eliminan el malware y cierran la brecha explotada.
5. **Recuperación**: los sistemas afectados y monitorizan cualquier anomalía adicional.
6. **Lecciones aprendidas**: documentan el incidente y actualizan sus procesos.

Hoy día, la gestión efectiva de incidentes es imprescindible debido al aumento de ataques avanzados y automatizados.

4.1 Estándares y marcos de referencia para la respuesta a incidentes

Los estándares y marcos de referencia proporcionan lineamientos estructurados que facilitan una respuesta eficiente y coordinada frente a incidentes de ciberseguridad.

A continuación, se presentan cinco de los marcos y estándares más reconocidos y utilizados internacionalmente para la gestión y respuesta a incidentes de ciberseguridad:

1. **NIST SP 800-61 Rev. 2 (Computer Security Incident Handling Guide)**

   Publicado por el Instituto Nacional de Estándares y Tecnología (NIST) de EE.UU., es uno de los referentes principales sobre gestión de incidentes y propone un ciclo de vida con fases como preparación, detección y análisis, contención, erradicación, recuperación y actividades post-incidente.

2. **ISO/IEC 27035**

   Este estándar internacional específico para la gestión de incidentes de seguridad de la información, proporciona directrices detalladas sobre el proceso desde la preparación hasta la mejora continua y es aplicable a todo tipo de organizaciones.

3. **NIST Cybersecurity Framework (CSF)**

   Aunque es más general para la gestión de riesgos de ciberseguridad, su estructura de cinco funciones (identificar, proteger, detectar, responder, recuperar), es ampliamente adoptada para diseñar planes de respuesta a incidentes y mejorar la resiliencia organizacional.

4. **SANS Incident Handler's Handbook**

   Creado por el SANS Institute, este marco es una referencia muy práctica y aplicada en la industria, detallando seis fases fundamentales: preparación, identificación, contención, erradicación, recuperación y lecciones aprendidas.

5. **Guía de Respuesta a Incidentes de CISA**

   La Agencia de Ciberseguridad e Infraestructura de EE.UU. (CISA) publica guías prácticas y adaptadas a sectores críticos, basadas en los principios de NIST, para orientar la preparación, detección, contención, recuperación y acciones post-incidente.

Ejemplo práctico: durante un ataque de ransomware, una empresa que implementa NIST SP 800-61 sigue protocolos ya estructurados, asigna roles y ejecuta pasos específicos de comunicación interna y externa, asegurando que ni el pánico ni la improvisación dominen la respuesta.

4.2 Políticas organizacionales de seguridad

Las políticas de seguridad son documentos alineados con la estrategia del negocio que establecen normas, responsabilidades y procedimientos para proteger los activos de información de una organización. Son requisito en la mayoría de marcos regulatorios e industriales.

A continuación, se presentan algunos ejemplos concretos de políticas de seguridad aplicables a diferentes plataformas, servicios y tecnologías actuales en las organizaciones:

Tabla 2. Ejemplos de Políticas organizacionales de seguridad ligadas a distintas tecnologías

Tecnología	Tipo de política	Ejemplo o descripción
Control de acceso.	Control de acceso basado en roles (RBAC).	Permite controlar el acceso a la información según el rol del usuario dentro de la organización.
Microsoft 365.	Protección contra amenazas (EOP).	Configuración de políticas EOP para antimalware, antispam y protección contra phishing en correos.
Microsoft Teams.	Prevención de pérdida de datos (DLP).	Reglas para evitar la exposición accidental de información crítica en Teams.
AWS IAM.	Política basada en identidad.	Solo permite acceso a recursos con autenticación multifactor (MFA).
AWS S3.	Control de acceso granular por bucket.	Acceso restringido de lectura/escritura a buckets

Tecnología	Tipo de política	Ejemplo o descripción
		específicos, denegando acceso sin MFA.
Computación en la nube.	Seguridad de datos en la nube.	Uso de cifrado en tránsito/reposo y controles Zero Trust; autenticación multifactor.
Firewall Manager de AWS.	Políticas de grupos de seguridad.	Gestión de acceso a recursos por reglas específicas en firewalls de AWS.
Microsoft Defender for Office 365.	Protección de cuentas prioritarias.	Configuración especial para proteger a directivos y cuentas de alto valor.
Acceso físico.	Control de acceso físico.	Uso de sistemas biométricos o tarjetas inteligentes para áreas sensibles.
Política organizacional general.	Uso de dispositivos BYOD.	Normas para el uso seguro y permitido de dispositivos personales en la red corporativa.

4.3 Rol del Centro de Operaciones de Seguridad (SOC)

El Centro de Operaciones de Seguridad o SOC por sus siglas en inglés, es un lugar —o un equipo— dentro de una empresa que se encarga de cuidar la seguridad informática. Es como el “equipo de vigilancia digital” que protege los sistemas, la información y los dispositivos de la organización frente a peligros como virus, hackers o fraudes.

Hay que pensar en el SOC como si fuera una central de control con cámaras y alarmas digitales, donde las personas que trabajan ahí vigilan todo lo que pasa dentro de las computadoras, redes y sistemas de la empresa. Si llega a pasar algo extraño, como un intento de robo de información o un comportamiento anormal en la red, ellos lo detectan y actúan rápidamente para detenerlo.

¿Qué hacen exactamente?

- Vigilan todo el tiempo (día y noche) para detectar si algo raro sucede con los sistemas.
- Investigan problemas, como archivos sospechosos o mensajes peligrosos, para saber si pueden causar daño.
- Responden a los ataques; es decir, los bloquean y ayudan a reparar todo lo que se haya visto afectado.
- Proponen mejoras en la seguridad, como nuevas reglas o herramientas para evitar problemas en el futuro.
- Ayudan a cumplir normas y proteger los datos que maneja la empresa.

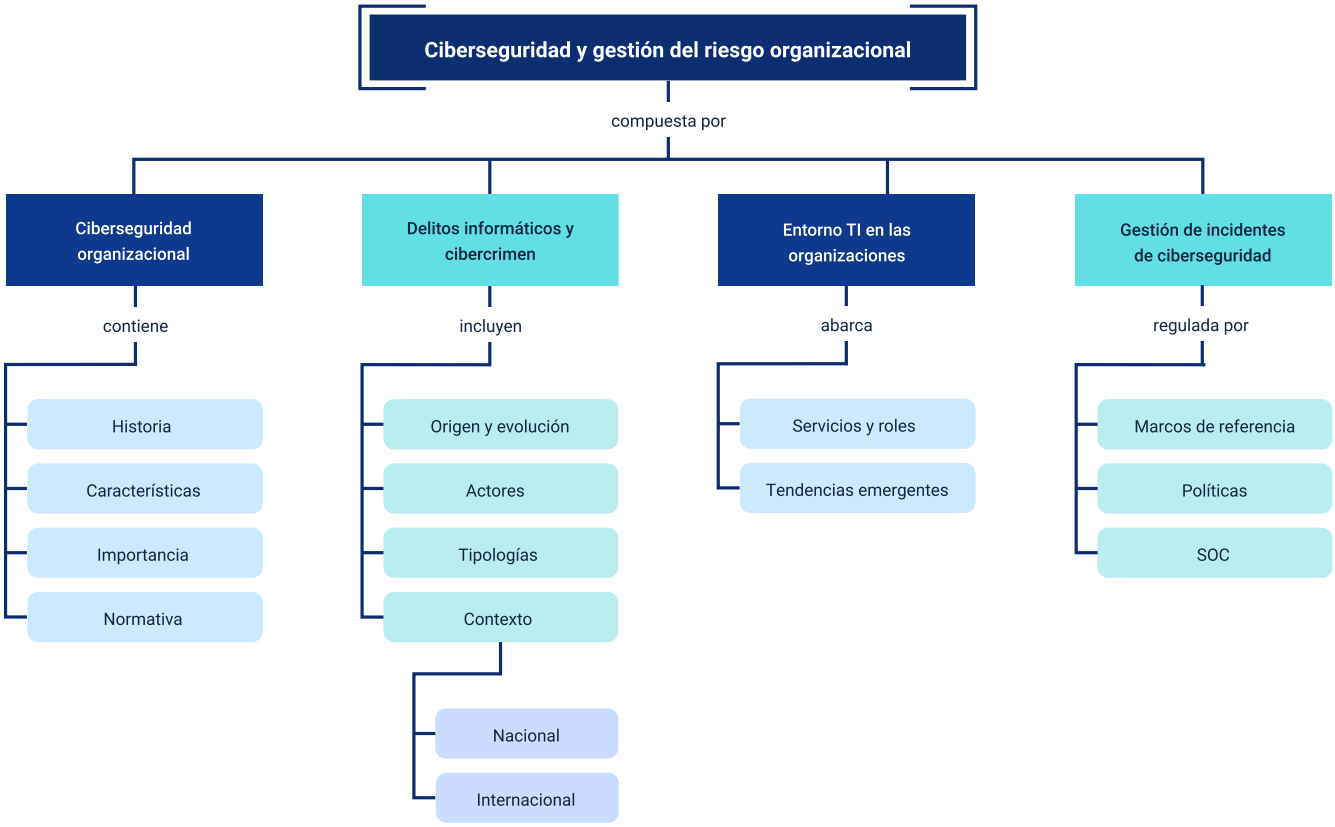
¿Por qué es importante?

Hoy en día, muchas cosas en las empresas se hacen con tecnología: correos electrónicos, archivos digitales, bancos en línea, videollamadas, entre otros. Si esa tecnología es atacada o deja de funcionar por un virus o un hacker, la empresa puede perder dinero, clientes o información muy valiosa. Por eso el SOC es muy importante: protege todo ese mundo digital para que las personas puedan trabajar seguras.

Con esta explicación, un estudiante sin conocimientos técnicos, puede entender que el SOC es, básicamente, el “equipo de seguridad digital” de una empresa que protege la información las 24 horas.

Síntesis

La ciberseguridad organizacional se puede resumir como un conjunto de estrategias, herramientas y políticas aplicadas por las empresas para proteger su información digital, frente a amenazas cibernéticas. En este componente, se detalló su evolución histórica, importancia empresarial y características como confidencialidad, integridad y disponibilidad, principios fundamentales de la ciberseguridad. También se abordó en profundidad los delitos informáticos, analizando su origen, actores involucrados, tipologías comunes como malware, phishing o ciberespionaje, marcos legales y desafíos internacionales frente al cibercrimen. El componente formativo, examinó además el entorno de tecnologías de la información en organizaciones, contemplando componentes como hardware, software y redes, así como roles técnicos y tendencias como inteligencia artificial, nube o IoT. Se explicó cómo se gestionan los incidentes de seguridad, mediante marcos reconocidos, remarcando la importancia de respuestas estructuradas y lecciones aprendidas. A su vez, se incluyeron ejemplos prácticos de políticas de seguridad para plataformas y se destacó el papel del SOC como centro neurálgico de vigilancia informática continua en las empresas. En conjunto, el componente formativo ofreció un panorama claro, actualizado y didáctico sobre los retos, mecanismos y actores involucrados en la protección de entornos digitales.


Ciberseguridad y gestión del riesgo organizacional
compuesta por
Ciberseguridad organizacional
Delitos informáticos y cibercrimen
Entorno TI en las organizaciones
Gestión de incidentes de ciberseguridad
contiene
incluyen
abarca
regulada por
Historia
Características
Importancia
Normativa
Origen y evolución
Actores
Tipologías
Contexto
Nacional
Internacional
Servicios y roles
Tendencias emergentes
Marcos de referencia
Políticas
SOC

Material complementario

Tema	Referencia	Tipo de material	Enlace del recurso
1.1 Concepto de ciberseguridad.	Ecosistema de Recursos Educativos Digitales SENA. (2022, 25 de octubre). La Ciberseguridad [Video]. YouTube.	Video.	https://www.youtube.com/watch?v=sk9dJtwZtlA&t=29s&ab_channel=EcosistemadeRecursosEducativosDigitalesSENA
1.4 Importancia de la ciberseguridad en el entorno empresarial.	Ecosistema de Recursos Educativos Digitales SENA. (2023, 1 de febrero). Introducción a la Ciberseguridad, sus fundamentos y normativa [Video]. YouTube.	Video.	https://www.youtube.com/watch?v=3rqfPRqnKIM&ab_channel=EcosistemadeRecursosEducativosDigitalesSENA
4. Gestión de incidentes de ciberseguridad.	Cyberzaintza. (2023, 22 de mayo). CSIRT.es Jorge Chinea, Responsable de Gestión de Incidentes y Crisis de Ciberseguridad	Video.	https://www.youtube.com/watch?v=j29xaVO7kTM&ab_channel=Cyberzaintza

Tema	Referencia	Tipo de material	Enlace del recurso
	en INCIBE [Video]. YouTube.		
4.2 Políticas organizacionales de seguridad.	Ecosistema de Recursos Educativos Digitales SENA. (2023, 6 de diciembre). Mejoramiento continuo de las estrategias de ciberseguridad [Video]. YouTube.	Video.	https://www.youtube.com/watch?v=pm9bgkdqRBg&ab_channel=EcosistemadeRecursosEducativosDigitalesSENA
4.3. Rol del Centro de Operaciones de Seguridad (SOC).	NSIT. (2021, 15 de marzo). NSIT ¿Cómo opera un SOC?	Video.	https://www.youtube.com/watch?v=-oiT4_y98YI&ab_channel=NSIT

Glosario

Amenaza: posible causa de un incidente que puede comprometer la seguridad de la información.

Centro de Operaciones de Seguridad (SOC): unidad especializada encargada de prevenir, detectar, analizar y responder a incidentes de ciberseguridad en tiempo real.

Cibercrimen: actividad delictiva llevada a cabo mediante medios digitales o informáticos.

Ciberseguridad: conjunto de prácticas, tecnologías y procesos encargados de proteger sistemas informáticos, redes y datos contra accesos no autorizados o daños.

Control de acceso: mecanismo que regula quién puede acceder a ciertos sistemas, información o recursos dentro de una organización.

Delito informático: cualquier acción ilegal que se comete utilizando tecnologías de la información o que está dirigida a ellas.

Incidente de seguridad: evento que compromete o tiene el potencial de comprometer la confidencialidad, integridad o disponibilidad de la información o los sistemas.

Infraestructura tecnológica: conjunto de componentes físicos y digitales (hardware, software, redes, servidores) que sustentan el funcionamiento de la tecnología de una organización.

Marco de referencia: conjunto de buenas prácticas, normas o metodologías que guían a las organizaciones en la gestión de la seguridad.

Política de seguridad: documento formal que define como una organización protege su información y sistemas frente a riesgos y amenazas.

Referencias bibliográficas

Armijo, M. (2011). Planificación estratégica e indicadores de desempeño en el sector público. Manual 69. Santiago de Chile, Chile: Naciones Unidas

Comunidad de Madrid. (s.f.) Tratamiento del riesgo. Comunidad de Madrid.

http://www.madrid.org/cs/StaticFiles/Emprendedores/Analisis_Riesgos/pages/pdf/metodologia/5TratamientodelRiesgo%28AR%29_es.pdf

David, F. (2008). Conceptos de Administración Estratégica. Ciudad de México, México: Ed. Pearson Prentice Hall, 11 edición.

Díaz, J. (2009). La importancia de Pensar Como Empresario.

https://www.negociosyemprendimiento.org/2009/07/la-importancia-de-pensar-como.html

Fred, D. (2008). Conceptos de Administración Estratégica. México. Pearson Prentice Hall.

Mendoza, A. (2005). Célebre Discurso de Steve Jobs en la Universidad de Stanford.

http://mercadeoglobal.com/blog/textos-del-celebre-discurso-de-steve-jobs-en-la-universidad-de-stanford/

Paredes, E. (2010). La Matriz FODA cruzada para ideas de negocio.

http://gestionando-empresas.blogspot.com/2010/08/la-matriz-foda-cruzada-para-ideas-de.html

Pick de Weiss, S. (1993). Planeando tu vida. México: Editorial Planeta.

Presidencia de la República de Colombia. (1971). Código de Comercio, Decreto 410 de marzo 27 de 1971.

https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=41102

Rogers, T. (2008). Cómo reforzar una mentalidad de pensamiento positivo.

https://es.wikihow.com/reforzar-una-mentalidad-de-pensamiento-positivo

Créditos

Nombre	Cargo	Centro de Formación y Regional
Milady Tatiana Villamil Castellanos	Responsable Ecosistema de Recursos Educativos Digitales (RED)	Dirección General
Diana Rocio Possos Beltrán	Responsable de línea de producción	Centro de Comercio y Servicios - Regional Tolima
Javier Eduardo Díaz Machuca	Experto temático	Centro de Comercio y Servicios - Regional Tolima
Andrés Felipe Velandia Espitia	Evaluador instruccional	Centro de Comercio y Servicios - Regional Tolima
Oscar Iván Uribe Ortiz	Diseñador web	Centro de Comercio y Servicios - Regional Tolima
José Jaime Luisa Tang Pinzón	Diseñador web	Centro de Comercio y Servicios - Regional Tolima
Diego Fernando Velasco Güiza	Desarrollador full stack	Centro de Comercio y Servicios - Regional Tolima
Veimar Celis Meléndez	Desarrollador full stack	Centro de Comercio y Servicios - Regional Tolima
Gilberto Junior Rodríguez Rodríguez	Animador y productor audiovisual	Centro de Comercio y Servicios - Regional Tolima
Norma Constanza Morales Cruz	Evaluadora de contenidos inclusivos y accesibles	Centro de Comercio y Servicios - Regional Tolima

Nombre	Cargo	Centro de Formación y Regional
Javier Mauricio Oviedo	Validador y vinculador de recursos educativos digitales	Centro de Comercio y Servicios - Regional Tolima