**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

| Programa de formación | Implementación de seguridad en internet de las cosas |
| --- | --- |

| Competencia | 220501110 - Implementar el sistema de seguridad de la información según modelo y estándares técnicos. | Resultado de aprendizaje | 220501110-01 - Establecer métodos de análisis y valoración de riesgos de seguridad en IoT de acuerdo con estándares internacionales y normatividad nacional.  220501110-02- Planificar el diseño de las estrategias de seguridad en IoT según el plan de tratamientos y matriz de riesgos informáticos. |
| --- | --- | --- | --- |

| Número del componente formativo | 01 |
| --- | --- |
| Nombre del componente formativo | Fundamentos de seguridad digital |
| Breve descripción | Los fundamentos necesarios para diagnosticar el estado actual de la ciberseguridad en una organización, adoptando métodos de análisis y valoración de riesgos son fundamentales para definir un plan de tratamiento adecuado. |
| Palabras clave | Activo de información, ciberseguridad, estándar, metodología, riesgo |

| Área ocupacional | 2 - Ocupaciones en ciencias naturales, aplicadas y relacionadas |
| --- | --- |
| Idioma | Español |

1. **TABLA DE CONTENIDO**

**Introducción**

**1. Amenazas cibernéticas en IoT**

1.1 *Malware* en IoT

1.2 Ataques DDoS

1.3 Contraseñas débiles o por defecto

* 1. Comunicaciones sin cifrado

1.5 Vulnerabilidades web

**2. Estándares de la seguridad IoT**

1. **INTRODUCCIÓN**

El concepto de internet de las cosas es bastante amplio, pero en realidad se refiere a dispositivos que son capaces de intercambiar datos con sistemas de cómputo, y estos dispositivos recopilan información sobre sistemas físicos por medio de sensores y se ejecutan acciones usando actuadores.

Para conocer un poco más sobre seguridad digital, es importante ver el siguiente video que dará una introducción al tema:



1. **DESARROLLO DE CONTENIDOS**
2. **Amenazas cibernéticas en IoT**

El IoT brinda un millar de beneficios, sin embargo, es bien importante generar confianza a los usuarios de IoT para que se sientan seguros y puedan controlar y obtener información de sus dispositivos conectados. Los desarrolladores de IoT deben preocuparse por proteger los dispositivos, autorizar y autenticarlos, actualizar los dispositivos en la medida de lo posible, asegurar la comunicación, garantizar la seguridad y privacidad de los datos, proteger las aplicaciones en la nube que se comunicaran con los dispositivos IoT, etc.

**Dispositivos IoT vulnerables**

Cualquier dispositivo conectado a internet puede ser utilizado para el montaje de ataques contra cualquier tipo de destino y servicio de internet así como a las redes internas.

**Figura 1**

*Conexión IoT*

Diagrama

Descripción generada automáticamente

A continuación, se presentan algunos dispositivos IoT vulnerables a ataques informáticos:



Muchos dispositivos IoT tienen capacidades limitadas de almacenamiento, memoria y procesamiento y requieren menos energía para funcionar; por ejemplo, cuando funcionan con baterías, luego se debe programar un cifrado y un descifrado en estos dispositivos y así es un poco más complejo para transmitir datos en forma segura.

En estos casos es conveniente hacer uso de múltiples capas de seguridad, poniéndolas, por ejemplo, en redes separadas y usar *firewalls* para balancear estas limitaciones.

Un ataque muy común es el [ataque de](https://en.wikipedia.org/wiki/Power_analysis) canal lateral, el cual se basa en el hecho de que cuando operan los criptosistemas estos causan efectos físicos como:

* La cantidad de energía que consume una operación.
* La cantidad de tiempo que lleva un proceso.
* El sonido que emite una operación.
* La radiación electromagnética filtrada por una operación.



**1.1** ***Malware* en IoT**

Una de las grandes amenazas de seguridad es el *software* malicioso o *malware* en IoT; aunque, y no menos importante entre otros programas de este tipo, están los troyanos, los gusanos y los *ransomware*. Por eso, el secuestro de computadores y portátiles es habitual para los usuarios y las empresas; sin embargo, los dispositivos IoT no almacenan información sensible, pero al cerrarlos sirve para realizar ataques que los pueden dejar inservibles.

Existe el concepto ***ransomware* de las cosas**, cuyo objetivo principal son los dispositivos como *hardware* de autos o cualquier otro dispositivo conectado a internet, drones y cámaras de seguridad

Es así como los peligros ocasionados por el *ransomware* pueden ser desastrosos, disruptivos o perjudiciales, propagándose a través de las redes e internet, comunicación inalámbrica como wifi o *bluetooth*.



Conozca algunos de los principales tipos de Malware:

Sabiendo esto, es momento de conocer algunos tipos de *malware*:



1.2 Ataques DDoS

En resumen, los ataques de *ransomware* son una amenaza muy peligrosa contra la tecnología operacional (OT) y los sistemas de control industrial (ICS), usados en empresas de alto nivel; son tan peligrosos estos ataques que están considerados como tal por la Agencia de Seguridad de Infraestructura y Ciberseguridad de Estados Unidos (CISA).

Por ejemplo, un ataque con *ransomware* puede afectar cadenas de suministro afectando la producción o robando información tecnológica.

**1.2 Ataques DDoS**

Son aquellos ataques que se realizan en red y sus siglas significan **Ataques de Denegación Distribuida de Servicio** (DDoS). Este tipo de ataque se aprovecha de la infraestructura que habilita los sitios web y los límites de capacidad específicos que se aplican a cualquier recurso de red, enviando varias solicitudes al recurso web atacado, con la intención de desbordar la capacidad de atención del sitio, obligándolo a administrar varias solicitudes y evitando que este funcione correctamente.

Los ataques más comunes de DDoS a algunos sitios *online* son: 

En el concepto de DDoS, entra la palabra ***botnet,*** que es una red conformada por equipos informáticos que han sido infectados con algún tipo de *malware* y que tiene el control de la información, obligando a enviar *spam*, propagando el virus o realizando ataques DDoS, sin el conocimiento o autorización de los usuarios propietarios reales de los dispositivos.

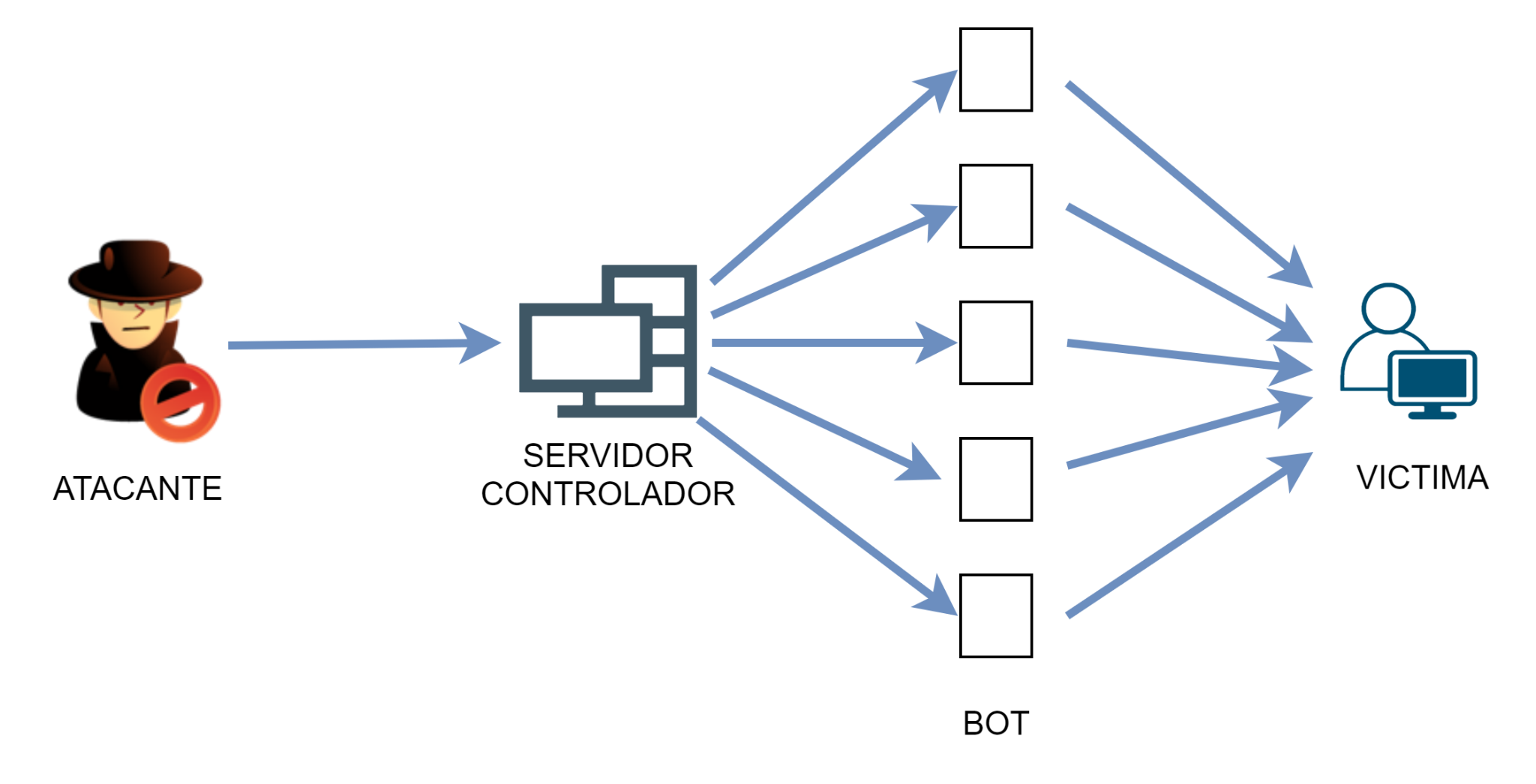
El *botnet* lo que hace es atacar usando DDoS enviando *spam* a los dispositivos, detecta contraseñas y distribuye *ransomware*. Este al ser un programa malicioso permite al cirberdelincuente tomar control del equipo afectado y es llamado también *bot* o programas zombies, dado que cumplen las órdenes de su amo; los *bots* toman el control del equipo, muchas veces sin que el propietario se dé cuenta de su presencia y realiza muchas tareas automatizadas.

Existen ***botnets*** compuestos por miles de objetos conectados a internet, los cuales tienen gran capacidad de generación de peticiones TCP/UDP suficiente para colapsar los recursos de cómputo de cualquier empresa. Una víctima en particular es sobrecargada con envíos de datos desde múltiples fuentes y como la víctima no es capaz de procesar tal cantidad de datos llegando al mismo tiempo, su sistema sufrirá caídas o parará de funcionar.

Un ejemplo es un ataque sobre un número telefónico de una víctima, donde esta es bombardeada con llamadas telefónicas por los *bots*, intentando conectarse a internet.

**Figura 2**

*Bot teléfonos*



**Funcionamiento de un ataque DDoS**

Cuando un negocio web sobrepasa los límites de capacidad de su infraestructura, debido a la cantidad de solicitudes, es muy probable que el nivel de servicio se vea afectado por alguna de las siguientes maneras:



Algunas formas de contrarrestar ataques con *botnets*, pueden ser:

* Examinar las características de los dispositivos IoT antes de comprarlos fijándose que cumplan con estándares y protocolos de seguridad.
* Mantener inventariado todos los dispositivos IoT y sus ubicaciones.
* Desarrollar y ejecutar planes de administración y aseguramiento de dispositivos IoT, incluyendo en este plan la vida útil de todos los dispositivos.
* Realizar segmentación de la red aislando los dispositivos de IoT y evitar que ese dispositivo sea utilizado por piratas informáticos en los sistemas de la empresa.

**1.3 Contraseñas débiles o por defecto**

Imagen que contiene objeto, pequeño, reloj, luz

Descripción generada automáticamenteMuchas de las vulnerabilidades son ocasionadas por malas prácticas al momento de asignar contraseñas a los dispositivos, los fabricantes de dispositivos o sistemas generalmente dejan una contraseña por defecto, la cual es conveniente que los usuarios la cambien voluntariamente o de manera forzada.

Los ciberdelincuentes prueban combinaciones de contraseñas hasta acertar, comprometiendo el *hardware* para futuros ataques.

Se debe, entonces, tener políticas de contraseñas robustas considerando longitudes mínimas, varios tipos de caracteres, política de renovación de contraseñas en forma periódica y no usar contraseñas anteriormente definidas.

Se recomienda la autenticación de dos factores (2FA), que requiere que el usuario emplee una contraseña y otra forma de autenticación como un código aleatorio generado a través de mensajes de texto SMS. Para las aplicaciones IoT se recomienda el uso de autenticación sensible al contexto (CAA) o autenticación adaptativa, donde se reconoce el dispositivo desde el cual se realizan intentos de acceso a una cuenta o dirección IP, detectando en forma automática cuántos de esos intentos son de riesgo alto usando métodos como *machine learning*.

Por lo anterior, es de suma importancia que conozca algunas formas de autenticación:



**1.4 Comunicaciones sin cifrado**

Una debilidad grande es la transmisión de datos entre dos dispositivos IoT, estos continuamente están transmitiendo información de todo tipo entre ellos y hacia los aplicativos en la nube. La transmisión de datos es una parte primordial de los dispositivos IoT, ya que un atacante puede tener acceso a la red local en donde están los dispositivos y acceder a información, revisar o modificar; es por ello que este tipo de ataque se llama **Hombre en el Medio** (MitM - *Man in the Middle*), lo que puede llegar a ser peligroso para las empresas e incluso para la vida de las personas

En términos de integridad, protección y encriptación de datos, los dispositivos *hardware* y *software* necesitan proveer un nivel de seguridad mínimo; de otra forma no será difícil que un intruso acceda a la información y la intercambie; viendo de esta manera como los atacantes entonces tendrán nuestros datos privados, información de dispositivos y controlarán los mismos.



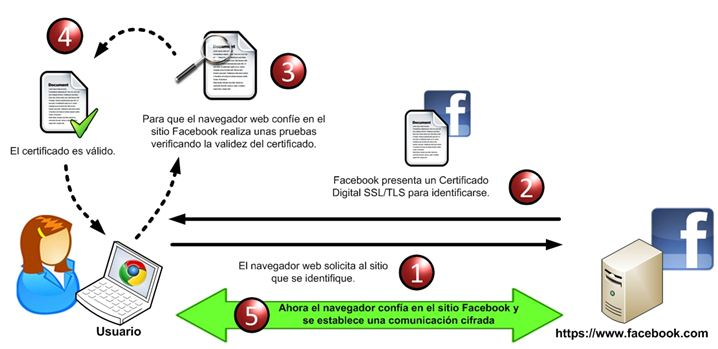
En comunicaciones cifradas se habla de protocolos SSL/TLS (*Secure Sockets Layer*) y (*Transport Layer Security*), estos protocolos permiten tener confianza al enviar información personal o privada a sitios web ocultando los datos, al usarse métodos de criptografía. Actualmente, esto es ampliamente usado en todos los sectores.

Es importante conocer algunos conceptos, como:



**Figura 3**

*Funcionamiento de SSL/TSL*

****

Retomando el último concepto expuesto y la imagen descrita, se puede ver que se hace referencia a un navegador que hace una petición al sitio seguro de Facebook; por ejemplo, este sitio envía un mensaje donde indica que va a establecer una conexión segura y sumnistra datos sobre la versión del protocolo SSL/TLS y otros parámetros para la conexión.

El servidor web, en este caso el de Facebook, responde con un mensaje informando que está de acuerdo en establecer una comunicación segura con los datos SSL/TLS proporcionados. Una vez que los dos conocen sus datos de conexión el servidor de Facebook envía su certificado digital al navegador web para identificarse como un sitio confiable.

Cuando tiene el certificado del sitio web de Facebook, realiza varias validaciones antes de confiar en el sitio, revisa la integridad del certificado, verifica que el certificado se encuentre correcto, descifrando la firma digital incluida en él mediante la clave pública de la AC y comparándola con la firma del certificado generado a la hora de consumir el sitio.

Además, revisa la vigencia del certificado, fecha de emisión, fecha de expiración y el emisor del certificado, haciendo uso de una lista de certificados raíz almacenados en la computadora y que contienen las claves públicas de las AC conocidas y de confianza. Si el navegador detecta que el certificado tiene inconsistencias presenta una alarma con este mensaje; cuando pasa todo esto entonces se establece una conexión segura entre sitio web y página web de usuario y al mismo tiempo, se traduce en seguridad para enviar datos sensibles.

**1.5 Vulnerabilidades web**

La forma más común como se interactúa con los dispositivos IoT es a través de aplicaciones web y bueno, es claro que es posible atacar una televisión con una inyección SQL o un XSS, por lo que es importante asegurar las interfaces de los usuarios como se hace con cualquier página web normal.

De aquí que es muy necesario seguir unas reglas sencillas pero fundamentales para evitar ataques a través de la web, como límites a intentos fallidos en el inicio de sesión de usuario, no almacenar datos sensibles innecesariamente y evitar fuga masiva de registros haciendo controles en los SQL,

Entre las vulnerabilidades más comunes tenemos:



Ahora bien, ya conociendo lo anterior, en el siguiente gráfico se presentarán algunos ataques cibernéticos registrados a lo largo del tiempo:



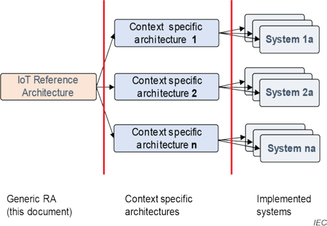
1. **Estándares de la seguridad IoT**

Si bien es cierto que el avance tecnológico en el internet de las cosas es tendencia de crecimiento a nivel mundial, aportando de forma importante al entorno empresarial, no se ha priorizado la seguridad de la información que viaja por los dispositivos,

Por ello, la Organización Internacional de Normalización presenta la arquitectura ISO/IEC 30141: 2018, la cual proporciona una arquitectura de referencia que se complementa con otros estándares internacionales para garantizar la seguridad y protección de los datos.

El estándar ISO / IEC 30141 es la primera arquitectura de referencia que tiene como objetivo hacer que el IoT sea eficiente, interrumpible, seguro y resistente a ataques.

Este estándar cuenta con un modelo conceptual y una arquitectura de referencia que permite utilizar un lenguaje común en todo el mundo para poder diseñar y desarrollar aplicaciones de IoT.



Para finalizar, se presentan algunas leyes colombianas aplicadas a seguridad y protección de datos:

****

1. **Síntesis**

Con el fin de relacionar el contenido de este componente formativo se presenta el siguiente cuadro de síntesis:



1. **ACTIVIDADES DIDÁCTICAS (opcionales si son sugeridas)**

| Descripción de actividad didáctica | |
| --- | --- |
| Nombre de la Actividad | Seguridad digital |
| Objetivo de la actividad | Reconocer las normas y estándares de seguridad de la información y la ciberseguridad. |
| Tipo de actividad sugerida |  |
| Archivo de la actividad  (Anexo donde se describe la actividad propuesta) | Anexos / CF01\_ActividadDidáctica |

1. **MATERIAL COMPLEMENTARIO**

| Tema | Referencia APA del Material | Tipo de material  (Video, capítulo de libro, artículo, otro) | Enlace del Recurso o  Archivo del documento o material |
| --- | --- | --- | --- |
| 1.1 Malware en IoT | CISA. (2021). *Rising ransomware threat to operational technology asserts*. <https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf> | Artículo | <https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf> |
| 1.2 Ataques DDoS | Incibe. (2017). *Dos mejor que uno: doble factor para acceder a servicios críticos*. <https://www.incibe.es/protege-tu-empresa/blog/dos-mejor-uno-doble-factor-acceder-servicios-criticos> | Artículo | <https://www.incibe.es/protege-tu-empresa/blog/dos-mejor-uno-doble-factor-acceder-servicios-criticos> |
| 1.4 Comunicaciones sin cifrado | Ramírez, L., D. O., y Espinosa, M., C. C (2018). *El cifrado web SSL/TLS*. <https://revista.seguridad.unam.mx/numero-10/el-cifrado-web-ssltls> | Artículo | <https://revista.seguridad.unam.mx/numero-10/el-cifrado-web-ssltls> |
| 2. Estándares de la seguridad IoT | ISO. (2018). *ISO/IEC 30141:20189.internet of Things (IoT)-Reference Architecture*. <https://www.iso.org/standard/65695.html> | Norma | <https://www.iso.org/standard/65695.html> |
| MinTIC. (2012). Ley estatutaria 181 de 2012. Protección de datos personales. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981> | Ley | <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981> |
| Función pública. (2008). Ley 1266 de 2008 Función pública.<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488> | Ley | <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34488> |
| Congreso de la República (2009). Ley 1273 de 2009. De la protección de la información y de los datos. <http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html> | Ley | <http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html> |
| ISO. (2018). *ISO/IEC 27000*. *Information technology - Security techniques - Information security management systems - overview and vocabulary* <https://www.iso.org/standard/73906.html> | Normas de seguridad | <https://www.iso.org/standard/73906.html> |
| ISO. (2009). *ISO/IEC 15408*. *Information technology - Security techniques - Evaluation criteria for IT security - part1: INtroduction and general model.* <https://www.iso.org/standard/50341.html> | Normas de seguridad | <https://www.iso.org/standard/50341.html> |
| ISO. (2013). *ISO/IEC 2002. Information technology - Security techniques - Code of practice for information security controls.* <https://www.iso.org/standard/54533.html> | Normas de seguridad | <https://www.iso.org/standard/54533.html> |

1. **GLOSARIO:**

| TÉRMINO | SIGNIFICADO |
| --- | --- |
| Auditoría | actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis representa adecuadamente la realidad que pretende reflejar o cumple con las condiciones que han sido acordadas en el nivel de servicio. |
| Auditorías internas de SGSI | el objetivo primordial de este tipo de auditoría de SGSI es averiguar si hay algo que se está realizando mal, de manera objetiva. El auditor interno debe ser una persona capacitada y atenta a lo que está ocurriendo en la empresa, debe poder descubrir si algo se hace mal dentro de su empresa de trabajo. Si se realiza un buen trabajo, correctivo o preventivo, entonces la auditoría interna de SGSI mejorará su seguridad. |
| Ciberseguridad | conjunto de metodologías, medidas y controles destinados a gestionar la seguridad de la información de una organización y/o de la información en general. |
| Seguridad informática | disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable. |

1. **REFERENCIAS BIBLIOGRÁFICAS:**

IBM. (2021). *Redes.* <https://www.ibm.com/co-es/cloud/learn/networking-a-complete-guide>

Oracle Corporation. (2010). *Modelo de referencia OSI (Guía de administración del sistema: servicios IP)*. <https://docs.oracle.com/cd/E19957-01/820-2981/ipov-8/index.html>

Rueda, R., J. S. (2021). El reto del desarrollo seguro de aplicaciones IoT en un mercado acelerado. *Revista Ingenio*, *18*(1), 54-61. <https://doi.org/10.22463/2011642x.2667>

1. **CONTROL DEL DOCUMENTO**

|  | Nombre | Cargo | Dependencia  *(Para el SENA indicar Regional y Centro de Formación)* | Fecha |
| --- | --- | --- | --- | --- |
| Autor (es) | Héctor Henry Jurado Soto | Experto Temático - Contratista | Regional Cauca – Centro de teleinformática y producción industrial | Marzo de 2022 |
| Caterine Bedoya Mejía | Diseñadora Instruccional | Regional Distrito Capital – Centro de Gestión Industrial | Marzo de 2022 |
| Andrés Felipe Velandia Espitia | Asesor Metodológico | Regional Distrito Capital – Centro de Diseño y Metrología | Marzo de 2022 |
|  | Rafael Neftalí Lizcano Reyes | Responsable Equipo Desarrollo Curricular | Regional Santander - Centro Industrial del Diseño y la Manufactura | Marzo de 2022 |
|  | José Gabriel Ortiz Abella | Corrector de estilo | Regional Distrito Capital – Centro de Diseño y Metrología. | Marzo del 2022. |

1. **CONTROL DE CAMBIOS**

**(Diligenciar únicamente si realiza ajustes a la Unidad Temática)**

|  | Nombre | Cargo | Dependencia | Fecha | Razón del Cambio |
| --- | --- | --- | --- | --- | --- |
| Autor (es) |  |  |  |  |  |