

Ciberseguridad

Módulo 1



1.1 Certificaciones de Seguridad

Certificaciones Teóricas

- ISO 27000

- Las normas que forman la serie ISO/IEC-27000 son un **conjunto de estándares creados y gestionados** por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrónica Internacional (IEC). Ambas organizaciones internacionales están participadas por multitud de países, lo que garantiza su amplia difusión, implantación y reconocimiento en todo el mundo.
- Las series 27000 están orientadas al **establecimiento de buenas prácticas en relación con la implantación, mantenimiento y gestión del Sistema de Gestión de Seguridad de la Información (SGSI)** o por su denominación en inglés Information Security Management System (ISMS).
- Estas guías tienen como objetivo **establecer las mejores prácticas en relación con diferentes aspectos vinculados a la gestión de la seguridad de la información**, con una fuerte orientación a la mejora continua y la mitigación de riesgos.
- ISO 27000: facilita las bases y lenguaje común para el resto de las normas de la serie.



1.1 Certificaciones de Seguridad

Certificaciones Teóricas

- ITIL
 - Las siglas ITIL significan Information Technology Infrastructure Library, que traduciríamos literalmente como Biblioteca de Infraestructura de Tecnologías de Información. ITIL es una **guía de buenas prácticas para la gestión de servicios de tecnologías de la información (TI)**. La guía ITIL ha sido elaborada para abarcar toda la infraestructura, desarrollo y operaciones de TI y gestionarla hacia la mejora de la calidad del servicio.

Los pilares de ITIL son los siguientes principios:

- **Procesos, necesarios para la gestión de TI** de acuerdo a la alineación de los mismos dentro de la organización.
- **Calidad**, entendida como la entrega a cliente del producto o servicio óptimos, es decir, incluyendo las características acordadas.
- **Cliente**, su satisfacción es el objetivo de la mejora de los servicios, siendo, por lo tanto el beneficiario directo de la implantación de las buenas prácticas de ITIL.
- **Independencia**, siempre deben mantenerse buenas prácticas a pesar de los métodos establecidos para cada proceso y de los proveedores existentes.

Cabe destacar que, para enfocar ese camino hacia la calidad del servicio, es necesario **contar con información fiable y segura**, ya que es imprescindible que ésta sea completa y precisa para la toma de decisiones



1.1 Certificaciones de Seguridad

Certificaciones Teóricas

- COBIT
 - [COBIT](#) es un marco de trabajo (framework) para el gobierno y la gestión de las tecnologías de la información (TI) empresariales y dirigido a toda la empresa.
 - Ha sido promovido por [ISACA](#) desde su primera versión en 1996 y actualmente se encuentra disponible la versión COBIT 2019. En la primera versión del marco de trabajo, COBIT se estableció como un acrónimo que significa Control Objectives for Information and Related Technology (Objetivos de Control para la Información y Tecnología Relacionada) y su público objetivo inicial eran los auditores de TI. La versión actual considera diversas partes interesadas, no solamente la función de TI de una empresa, sino a otros interesados como la Junta Directiva, Dirección Ejecutiva, Auditoría, etc.



CISSP

- Certification for Information System Security Professional (CISSP) es una certificación de proveedor neutral, que refleja las aptitudes de los profesionales de seguridad de la información, con una medición objetiva de capacidades.
- La certificación CISSP significa que el profesional de seguridad de la información **demuestra un conocimiento práctico de la seguridad de la información**, confirma el compromiso con la profesión y establece un estándar de mejores prácticas.
- ESTÁNDARES Y CERTIFICACIÓN CISSP
- La certificación Certified Information Systems Security Professional (CISSP) está acreditada por el ANSI (Instituto Nacional Estadounidense de Estándares) según la Norma ISO (Organización Internacional de Normalización) 17024: 2003. El examen CISSP consta de 250 preguntas de opción múltiple, que cubren temas como **sistemas de control de acceso, criptografía y prácticas de gestión de seguridad**, y es administrado por el Consorcio Internacional de Certificación de Seguridad de Sistemas de Información o (ISC) 2.
- CONCENTRACIÓN CISSP
- Con la evolución continua de la seguridad de la información, (ISC) 2 ofrece credenciales concentradas, llamadas Concentraciones CISSP. Aprobar un examen de concentración CISSP demuestra que el profesional de seguridad de la información tiene capacidades comprobadas y experiencia en la materia más allá de lo que se requiere para la credencial CISSP. Están disponibles en las siguientes áreas:
 - **Arquitectura (CISSP-ISSAP)**
 - **Ingeniería (CISSP-ISSEP)**
 - **Gestión (CISSP-ISSMP).**



CISA



- Las siglas CISA corresponden a Certified Information Systems Auditor, o lo que es lo mismo, se trata de una **certificación para auditores** que tiene reconocimiento a nivel mundial. La CISA cuenta con el respaldo de la Asociación de Control y Auditoría de Sistemas de Información (ISACA) y, para poder obtener dicha certificación, hay que cumplir una serie de requisitos impuestos por este organismo.
- A través de la certificación CISA se reconocen los conocimientos y aptitudes de un profesional en diferentes áreas establecidas. Es el caso de la **auditoría en sistemas de información, las operaciones, soporte y mantenimiento de estos sistemas, el gobierno y mantenimiento de la tecnología de la información, la protección de la información y finalmente, la adquisición, ejecución y desarrollo de estos sistemas** a los que estamos haciendo referencia. Todos aquellos que quieran convertirse en un CISA podrán demostrar que son capaces de evaluar las vulnerabilidades de dichos sistemas, elaborar informes, establecer controles y por supuesto mostrar las habilidades y conocimientos en auditorías, así como dar a conocer su experiencia dentro de este sector.
- ¿Por qué se creó la certificación CISA?
- La Certified Information Systems Auditor se creó en el año 1978 y fueron muchos los motivos que se establecieron para que finalmente la CISA comenzara a funcionar. Hay que destacar que esta certificación era necesaria para poder contar con una herramienta que motivara a los auditores de este tipo de sistemas. Así, podrían mantener sus habilidades y demostrar que los programas de mantenimiento pueden ser efectivos. Así mismo, la CISA fue creada para poder desarrollar una herramienta que se utilice como método de evaluación para aquellos profesionales que se dediquen a realizar auditorías de los sistemas de información. Y, por último, esta certificación existe con la intención de poder suministrar ayuda y criterios de gestión para seleccionar a los desarrolladores y al personal en general.
- Para poder conseguir esta certificación hay que pasar un examen. El primero de ellos se llevó a cabo en el año 1981 y poco a poco se ha vuelto muy popular y ha ido creciendo. Actualmente, un examen CISA se lleva a cabo en más de 200 lugares repartidos por todo el planeta y se establece en 11 idiomas diferentes. Si se supera el examen el Departamento de Defensa de los Estados Unidos, dentro de la categoría de Aseguramiento de Información Técnica, es el encargado de aprobar de manera oficial la certificación.
- ¿Cuáles son los requisitos que hay que cumplir?
- Las personas que quieran acceder a la CISA tienen que superar un examen que se basa en el Código Profesional de Ética de ISACA. Los principales requisitos para poder presentarse son que el candidato cuente con más de 5 años de experiencia, tanto en control de seguridad informática como interno, así como en la elaboración de auditorías. También hay que contar con un programa formativo de manera continuada. Si no se cumplen estos requisitos, ISACA establece algunas equivalencias que pueden servir para realizar el examen. Así, también podrán presentarse los que cuenten al menos con un año de experiencia en auditorías operaciones o sistemas de información, o los que tengan de 60 a 120 horas en estudios profesionales que se pueden sustituir por uno o dos años de experiencia en el sector. Otra opción es haber estado durante dos años ejerciendo como instructor a tiempo completo en la Universidad, siempre en materia relacionada con este sector

CRISC

- Introducida en el año 2010, la CRISC | Certified in Risk and Information Systems Control es una nueva certificación ofrecida por ISACA y se basa en la **propiedad intelectual de la asociación**, investigación de mercado independiente y los aportes de expertos en la materia de todo el mundo. La certificación ha sido diseñada para profesionales de TI y de negocios **que identifiquen y gestionen los riesgos mediante la elaboración, implementación y mantenimiento de sistemas adecuados de información de los controles.**

La certificación CRISC está diseñada para cumplir con la demanda creciente de profesionales, que puedan integrarse a la **administración de riesgo de la empresa (ERM)**, con habilidades en controles discretos de SI.

- Las habilidades técnicas y prácticas que promueve y evalúa la certificación CRISC, son los pilares sobre los que se cimienta el éxito en este campo creciente y la certificación CRISC demuestra pericia y experiencia en este rol.

La certificación CRISC reconoce a los profesionales que tienen amplia experiencia en la gestión integral de riesgos relativos a las tecnologías de la información. Asimismo, reconoce a los profesionales especialistas en el diseño, implementación y evaluación de controles para los sistemas de información.



**Certified in Risk
and Information
Systems Control®**
An ISACA® Certification

CISM

- La certificación CISM (Certified Information Security Manager) de la asociación ISACA (Information Systems Audit and Control Association) ha sido desarrollada para los profesionales que se dedican a la gestión de la seguridad de la información. Esta define los conocimientos y las competencias para que estos profesionales sean capaces de diseñar, supervisar, evaluar y administrar la seguridad de la información de una organización. ¿Quieres saber más sobre la certificación CISM y cuál es su importancia? En UNIR abordamos los puntos clave de esta certificación de seguridad informática.
- 1. Gobierno de la seguridad de la información
- 2. Gestión de riesgos de la información
- 3. Desarrollo y gestión del programa de seguridad de la información
- 4. Gestión de incidentes de seguridad de la información



Certificaciones Prácticas

1.2 recursos en la Web

1. Software antivirus.

- En cualquier caso, todos los computadores conectados a la red, personales y corporativos, deben contar con un antivirus gratuito y confiable. Este tipo de programas permite contar con medidas de protección efectivas ante la detección de malware u otros elementos maliciosos, por medio de ofrecer la posibilidad de eliminar las posibles amenazas o poner al dispositivo en estado de “cuarentena”.
- Dentro del mercado, existen soluciones que integran diferentes funcionalidades adaptables a las necesidades de cada organización. Sin embargo, es importante que la que se adopte cuente con las actualizaciones pertinentes para así no quedar caducas ante nuevas amenazas.

2. Firewall perimetral de red.

- Es una de las herramientas de ciberseguridad más recomendadas. Su funcionamiento es simple: escanea los paquetes de red, permitiéndoles o bloqueándolos según las reglas definidas por un administrador.
- Si bien es cierto que su estructura es básica si se compara a la sofisticación de las amenazas, se pueden encontrar firewalls modernos que pueden clasificar los archivos utilizando varios parámetros. Así, se puede inspeccionar con eficiencia el tráfico web, identificar a usuarios, bloquear el acceso que no está autorizado, entre otras acciones.

3. Servidor proxy.

- Un proxy es un dispositivo o programa informático que actúa como intermediario entre las conexiones del navegador e Internet, filtrando todos los paquetes entre ambos. Está catalogada como una de las buenas herramientas de seguridad informática debido a que, por medio de ella, se puede bloquear sitios web que se estimen como peligrosos o prohibidos dentro del ambiente laboral.
- Por otro lado, permite establecer un sistema de autenticación, el cual limita el acceso a la red externa, permitiendo contar con registros sobre sitios, visitas, entre otros datos.

4. Cifrado de punto final o end point disk encryption.

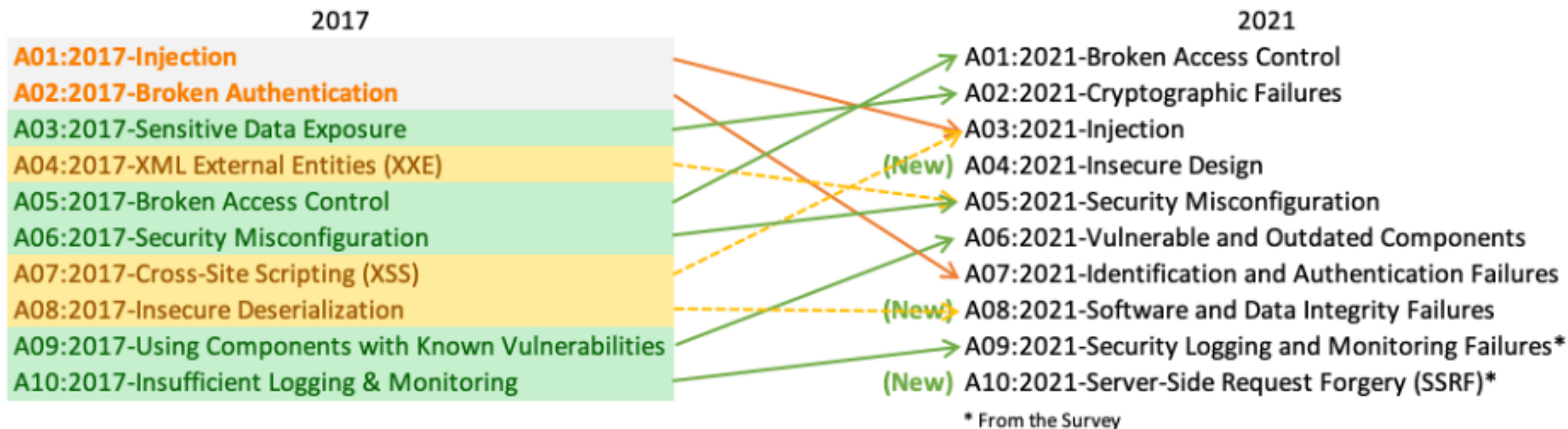
- Es un proceso de codificación de datos para que no pueda ser leído o utilizado por nadie que no tenga la clave de descifrado correcta. En esencia, protege los sistemas operativos de la instalación de archivos de arranque corruptos, bloqueando los archivos almacenados en computadores, servidores, entre otros puntos finales.

5. Escáner de vulnerabilidades.

- Es una de las herramientas de seguridad en sistemas informáticos fundamentales en las empresas de cualquier tamaño. Consiste en un software que se encarga de detectar, analizar y gestionar los puntos débiles del sistema.
- Gracias a esta plataforma, se puede mantener controlada la exposición de los recursos empresariales a las amenazas de ciberseguridad y sus posibles consecuencias. Además, permite alertar en tiempo real, lo que ayuda a la solución de problemas de forma oportuna y sin comprometer la continuidad del negocio.

- <https://docs.microsoft.com/en-us/microsoft-365/security/intelligence/safety-scanner-download?view=o365-worldwide>

Top ten de riesgos de seguridad para aplicaciones web 2021



1.3 Conceptos Generales de Seguridad

1.3.1 Terminología

• 1.3.2 Malware

- [Malware](#) o “software malicioso” es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas.
- El malware hostil, intrusivo e intencionadamente desagradable intenta **invadir, dañar o deshabilitar** ordenadores, sistemas informáticos, redes, tabletas y dispositivos móviles, a menudo asumiendo el control parcial de las operaciones de un dispositivo. Al igual que la gripe, interfiere en el funcionamiento normal.
- La intención del malware es **sacarle dinero al usuario ilícitamente**. Aunque el malware no puede dañar el hardware de los sistemas o el equipo de red, **sí puede robar, cifrar o borrar sus datos, alterar o secuestrar funciones básicas del ordenador y espiar su actividad en el ordenador sin su conocimiento o permiso**.



1.3.3 Métodos de Ataque

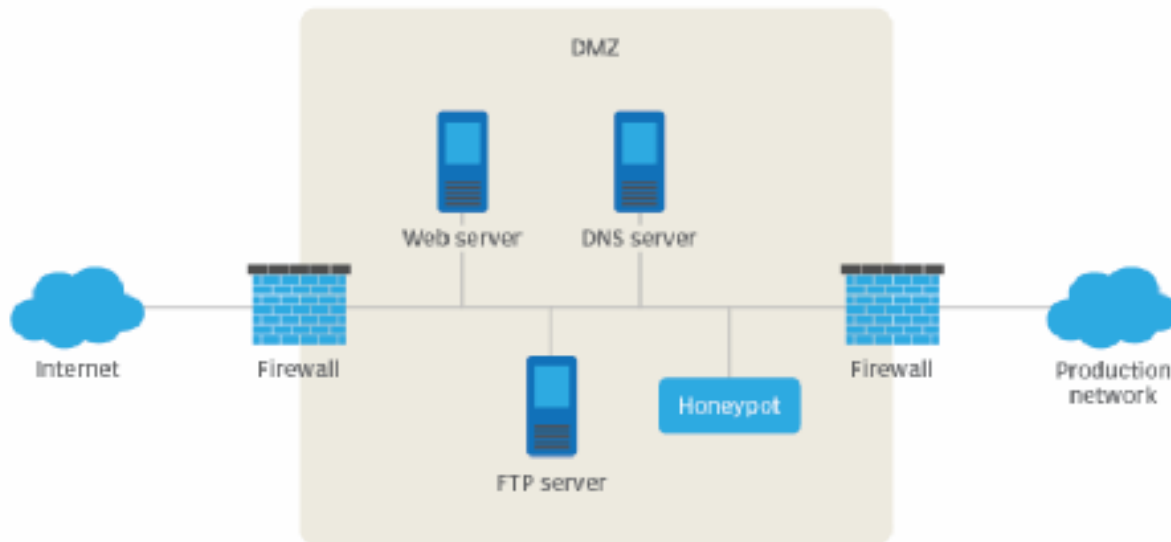
Principales causas que pueden generar un ataque cibernético se destacan:

1. **Vulnerabilidad de los sistemas informáticos**, es decir, fallas o deficiencias que ponen en riesgo los activos al no estar protegidos de manera efectiva.
2. **Divulgación de información confidencial** por parte de los empleados de forma accidental.
3. **Pérdida y robo de dispositivos electrónicos** que almacenan información privada de la empresa.
4. **Empleados con malas intenciones y sin escrúpulos** que ponen en riesgo la información de la empresa.
5. **Brechas o falta de controles por parte de terceros**, es decir, si estos son víctimas de un ataque, los ciberdelincuentes pueden acceder a información de otras empresas con las que tienen relaciones y buscar la manera de también perjudicarlas.
6. **Ingeniería social, social engineering**, que consiste en la manipulación de personas específicas con el fin de obtener datos confidenciales como contraseñas u otros de gran valor e importancia para la empresa.



1.3.4 Honeypot

A honeypot's place in the network

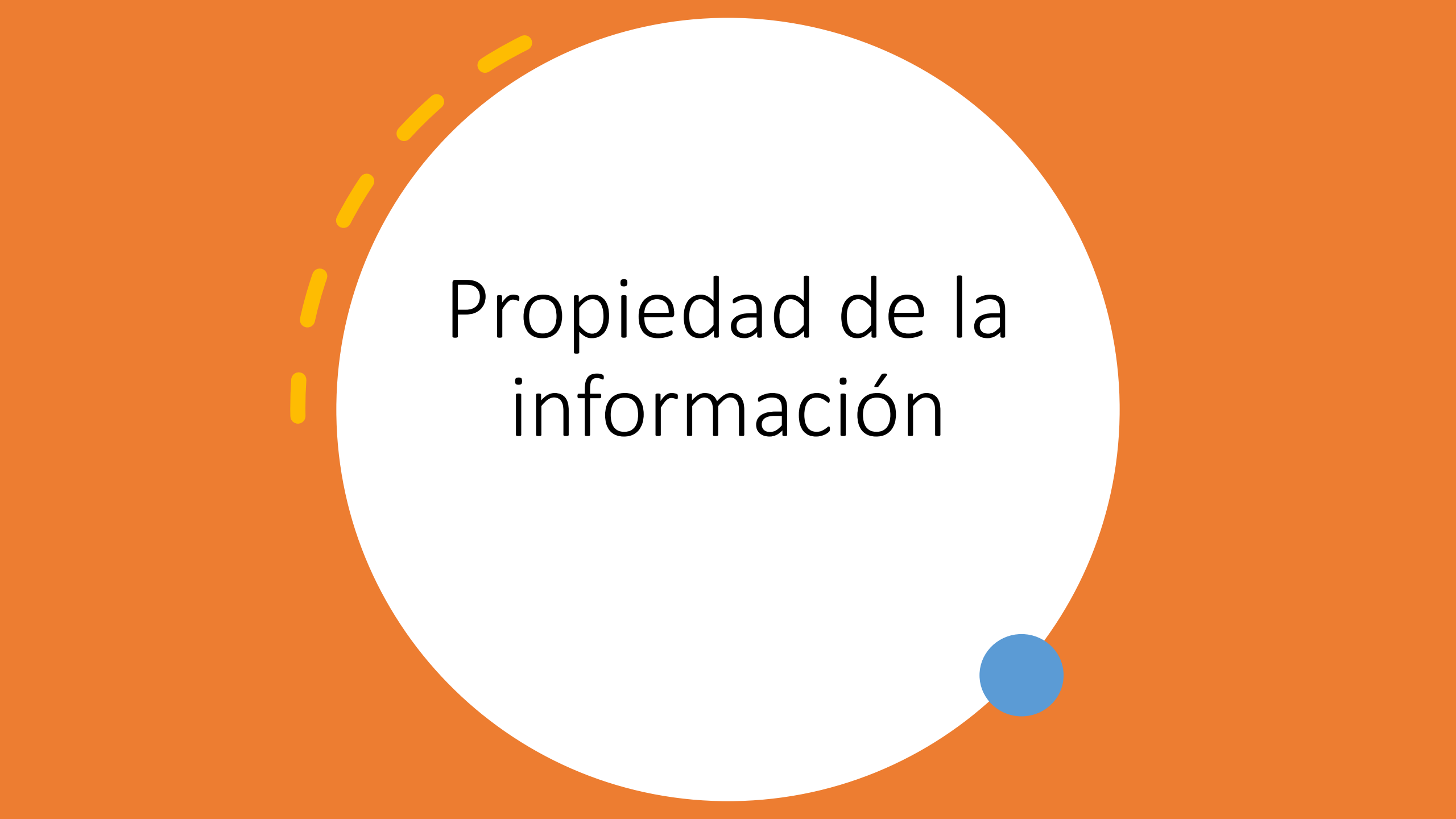


- Los HoneyPots son un tipo de herramientas que **simulan servicios y/o aplicaciones, normalmente vulnerables**, en un entorno controlado para registrar y analizar cualquier tipo de actividad que pueda infundir sospecha.
- Se trata de atraer a posibles atacantes para analizar los ataques realizados contra los servicios y aplicaciones simulados. Ahí está el verdadero objetivo de los HoneyPost; el estudio de las técnicas de ataque para optimizar y reforzar las medidas de seguridad del entorno, digamos, productivo o real, de nuestra infraestructura informática / sistemas / red. Además, al ser los HoneyPots sistemas que atraen a los atacantes, es posible «distrarlos» para que no interfieran en el entorno real productivo, es por ello, y tal como os he apuntado, que el entorno HoneyPot debe estar protegido, separado del entorno real.

1.3.5 Rootkits



- Un rootkit es un término que se aplica a un tipo de malware, diseñado **para infectar un PC**, el cual permite al hacker instalar diferentes herramientas que le dan acceso remoto al ordenador. Este malware se oculta en la máquina, dentro del sistema operativo y sortea los obstáculos como aplicaciones antimalware o algunos productos de seguridad.
- El rootkit contiene diferentes herramientas maliciosas como un
 - keylogger, un módulo para robar los números de tarjeta o cuentas bancarias,
 - un bot para ataques DDoS y otras funciones que pueden desactivar el software de seguridad.
- Los rootkits actúan como un backdoor que permite al atacante infectar, de forma remota, al equipo y eliminar o instalar componentes específicos.



Propiedad de la información

1.3.6 Confidencialidad

- La confidencialidad es la propiedad que **impide la divulgación de información a individuos, entidades o procesos no autorizados**. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.
 - La pérdida de la confidencialidad de la información puede adoptar muchas formas.
 - Cuando alguien mira por encima de su hombro, mientras usted tiene información confidencial en la pantalla,
 - cuando se publica información privada,
 - cuando un laptop con información sensible sobre una empresa es robado,
 - cuando se divulga información confidencial a través del teléfono, etc.

Todos estos casos pueden constituir una violación de la confidencialidad.

1.3.7 Integridad

- **Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.** (No es igual a integridad referencial en bases de datos.) A grandes rasgos, la integridad es mantener con **exactitud la información tal cual fue generada**, sin ser manipulada ni alterada por personas o procesos no autorizados.
- La integridad también es la propiedad que busca proteger que se modifiquen los datos libres de forma no autorizada, para salvaguardar la precisión y completitud de los recursos.
- La violación de integridad se presenta cuando un empleado, programa o proceso (por accidente o con mala intención) modifica o borra datos importantes que son parte de la información.
- La integridad garantiza que los datos permanezcan inalterados excepto cuando sean modificados por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad.
- La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad: **la firma digital es uno de los pilares fundamentales de la seguridad de la información.**

1.3.8 Disponibilidad

- La disponibilidad **es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones**. A grandes rasgos, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.
- En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizados para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente. **La alta disponibilidad sistema objetivo debe estar disponible en todo momento**, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones del sistema.
- **Garantizar la disponibilidad implica también la prevención de ataque de denegación de servicio**. Para poder manejar con mayor facilidad la seguridad de la información, las empresas o negocios se pueden ayudar con **un sistema de gestión** que permita conocer, administrar y minimizar los posibles riesgos que atenten contra la seguridad de la información del negocio.
- La disponibilidad además de ser importante en el proceso de seguridad de la información, es además variada en el sentido de que existen varios mecanismos para cumplir con los niveles de servicio que se requiera.
- Tales mecanismos se implementan en
 - infraestructura tecnológica,
 - servidores de correo electrónico,
 - de bases de datos,
 - de web etc,

mediante el uso de clusters o arreglos de discos, equipos en alta disponibilidad a nivel de red, servidores espejo, replicación de datos, redes de almacenamiento (SAN), enlaces redundantes, etc. La gama de posibilidades dependerá de lo que queremos proteger y el nivel de servicio que se quiera proporcionar.

1.3.10 Autenticación



ES LA PROPIEDAD QUE **PERMITE IDENTIFICAR EL GENERADOR DE LA INFORMACIÓN**. POR EJEMPLO AL RECIBIR UN MENSAJE DE ALGUIEN, ESTAR SEGURO DE QUE ES DE ESE ALGUIEN EL QUE LO HA MANDADO, Y NO UNA TERCERA PERSONA HACIÉNDOSE PASAR POR LA OTRA (SUPLANTACIÓN DE IDENTIDAD).



EN UN SISTEMA INFORMÁTICO SE SUELE CONSEGUIR ESTE FACTOR CON EL USO DE CUENTAS DE USUARIO Y CONTRASEÑAS DE ACCESO.



ESTA PROPIEDAD SE PUEDE CONSIDERAR COMO UN ASPECTO DE LA INTEGRIDAD -SI ESTÁ FIRMADO POR ALGUIEN, ESTÁ REALMENTE ENVIADO POR EL MISMO-

1.3.9 Non-Repudiation

El no repudio o irrenunciabilidad **proporciona garantía al receptor de una comunicación en cuanto que el mensaje fue originado por el emisor y no por alguien que se hizo pasar por este.** Además, previene que el remitente o emisor del mensaje afirme que él no envió el mensaje.

En resumen, el no repudio en seguridad de la información **es la capacidad de demostrar o probar la participación de las partes (origen y destino, emisor y receptor, remitente y destinatario), mediante su identificación, en una comunicación o en la realización de una determinada acción.**

Para garantizar el no repudio en seguridad informática se necesitan establecer los siguientes mecanismos:

- Identificación: mecanismo o proceso que provee la capacidad de identificar a un usuario de un sistema.
- Autenticación: permite verificar la identidad o asegurar que un usuario es quien dice ser.

Se suele aplicar a:

- Contratos formales establecidos de manera telemática.
- Comunicación entre dos partes.
- Transferencia de datos.
- Acciones de los usuarios en un sistema informático.

Tipos de no repudio

- En origen: consiste en garantizar que una persona envió un determinado mensaje. El remitente no puede negar que lo mandó, ya que el destinatario dispone de pruebas del envío.
- En destino: avala que alguien recibió un determinado mensaje. En este caso, el destinatario no podrá rebatir que no lo recibió porque el remitente cuenta con pruebas de la recepción.

Ejemplos

- Tipos de firma electrónica
- Los distintos tipos de firma electrónica son:
 - Simple
 - Se trata de aceptar o rechazar el contenido de un documento, son típicas en las condiciones generales de uso, políticas de seguridad o privacidad...
 - Avanzada OTP
 - La persona firmante recibe un código a través de un canal de comunicaciones distinto al de la operativa de firma (p. ej. móvil o correo electrónico) al momento de firmar. Es típica su utilización en compras electrónicas u operaciones de banca electrónica.
 - Biométrica
 - La persona firma físicamente en una tablet o dispositivo electrónico. Se utiliza, por ejemplo, en el servicio de correo o transporte de paquetería, en las sucursales bancarias...
- Certificado digital
 - Se firma mediante un certificado que se apoya en un par de claves, una privada y una pública. Hay que aclarar que certificado digital no es lo mismo que firma electrónica. El certificado digital es un documento que nos identifica en internet para poder realizar trámites online y que permite la firma electrónica. Ejemplos de firma electrónica serían la firma realizada mediante el DNI electrónico o con los certificados digitales de persona física de la FNMT.

1.3.11 Clasificación de la Información

- La información es poder, y según las posibilidades estratégicas que ofrece tener acceso a cierta información, ésta se clasifica como:
 - Crítica:
 - Es indispensable para la operación de la empresa.
 - Valiosa:
 - Es un activo de la empresa y muy valioso.
 - Sensible:
 - Debe de ser conocida por las personas autorizadas.

Los ciberataques más comunes son:

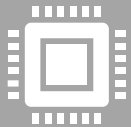
1. **Phishing y spear phishing.** El *phishing* consiste en correos electrónicos o mensajes de texto que aparentemente son enviados por fuentes confiables y que persuaden al destinatario a completar una acción, abrir un enlace malicioso, que va a poner en riesgo la información personal o de la empresa.

Y el *spear phishing* busca obtener datos de valor dirigiéndose a una persona o empresa específica luego de haberse ganado su confianza. Este ataque es muy utilizado con empresas y personas reconocidas.
2. **Whaling o "caza de ballenas".** Están dirigidos a perfiles directivos como CEO's o CFO's y otros cargos altos de las organizaciones con el objetivo de robarles información confidencial a la que ellos tienen acceso.
3. **Malware.** Se trata de un programa o código malicioso que afecta de manera secreta y silenciosa a un sistema de información. Un *malware* tiene la capacidad de irrumpir, perjudicar y deshabilitar los ordenadores y demás activos de información, en otras palabras, a través de este se pueden robar y borrar datos, secuestrar funciones y espiar actividades sin ser notados. Algunos malware son los *ransomware*, troyanos y spyware.
4. **Ransomware.** También conocido como secuestro de datos consiste en el bloqueo, por parte de un hacker, de un dispositivo electrónico y en la encriptación de los archivos para que el usuario dueño no pueda acceder a la información y datos almacenados.
5. **Inyección SQL.** Es un ataque a la web que consiste en la infiltración de un código malicioso que aprovecha errores y vulnerabilidades de una página web. Es utilizado para robar bases de datos, manipular o destruir información.

1.4 Frameworks de Seguridad y Estándares



El Framework de Ciberseguridad es un conjunto predefinido de **políticas y procedimientos** definidos por las principales organizaciones de ciberseguridad para **mejorar las estrategias de seguridad cibernética en un entorno empresarial**, y está documentado para el **conocimiento teórico y los procedimientos de implementación práctica**.



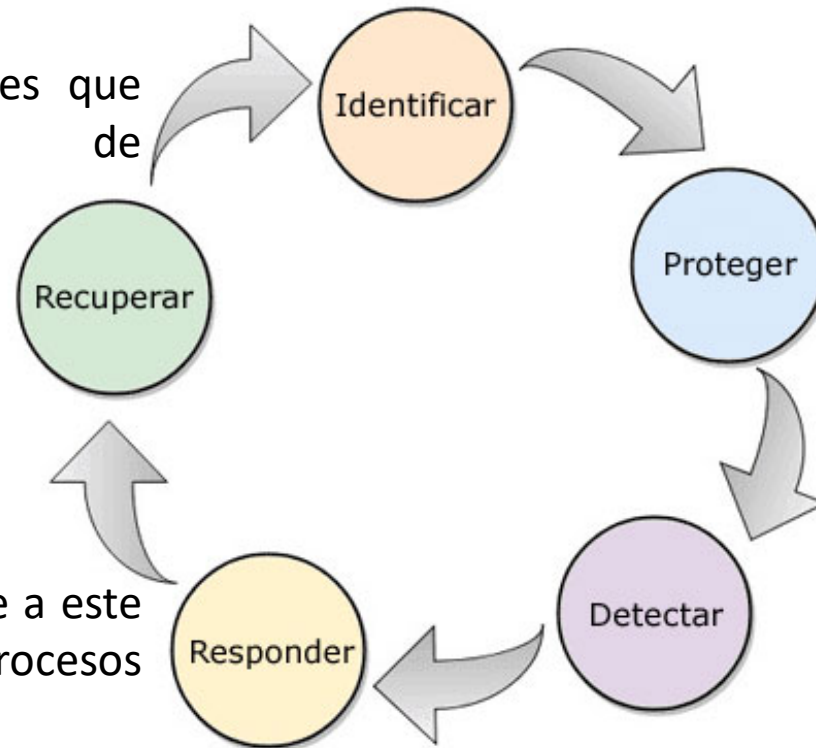
Se diseñan, a veces, dirigidos a una industria específica y están diseñados para **reducir las vulnerabilidades desconocidas y las configuraciones erróneas existentes dentro de una red empresarial**. Es decir, digamos que el Framework de Ciberseguridad es un plan para enriquecer la seguridad informática de su empresa.

Estrategias del Framework de Ciberseguridad

Los cinco procesos principales que definen el Framework de Ciberseguridad son:

1. Identidad
2. Protección
3. Detección
4. Respuesta
5. Recuperación

Cualquiera funcionará en base a este proceso. Definamos estos procesos uno por uno.



Identificar:

Esta función ayuda a la organización a identificar los **puntos de contacto cibernéticos existentes en un entorno empresarial**. Pueden ser activos de TI, recursos, información y más.

Proteger: Este se encarga del **control de acceso corporativo, la seguridad de los datos y el mantenimiento** para cuidar la ciberseguridad en y alrededor del entorno empresarial. Lo más probable es que sea una fase proactiva de la ciberseguridad empresarial.

Detectar:

Esta función es donde una organización **identificará posibles infracciones mediante la supervisión de los registros** y el cuidado de los procedimientos de detección de intrusos a nivel de red y dispositivo. La información de seguridad y la gestión de eventos están cubiertas por este procedimiento.

Responder:

Una vez que se detecta la infracción, las organizaciones deben encargarse del procedimiento de respuesta: **comprender la infracción, corregir la vulnerabilidad y continuar con la recuperación**.

La mitigación, la planificación de la respuesta y las mejoras se manejarán en esta etapa.

Recuperar:

Los procedimientos de recuperación, como el **sistema de recuperación de desastres y los planes de respaldo**, se manejarán en esta etapa de la estrategia del Framework de Ciberseguridad.

Tipos de Frameworks de Ciberseguridad

- ISO 27001/27002
 - La Organización de Normas Internacionales (ISO) fue la que desarrolló ISO27000, que cubre todos los aspectos generales del Framework de Ciberseguridad que se puede aplicar a las empresas de cualquier vertical.
 - Considerado como un equivalente a las normas ISO 9000 para la fabricación, ayuda a las organizaciones a definir y medir la calidad de la ciberseguridad existente en su entorno.
 - ISO2700 define una visión general, mientras que ISO27001 se encarga de los requisitos, e ISO27002 se encarga de los procedimientos de implementación.
 - Junto con la lista de estándares anterior, la norma ISO 27799 define la seguridad perteneciente a la industria de la salud.
- Controles de Seguridad CIS
 - El Centro de Seguridad de Internet (CIS) ha definido un conjunto de controles de seguridad críticos que las organizaciones deben establecer dentro de su red para lograr un Framework y estrategias de ciberseguridad eficaces.
 - CIS ha definido tres conjuntos de Controles de Seguridad Críticos, que son básicos, fundamentales y organizativos, y cuenta con 20 controles en total. Abordan varios controles de seguridad que deberían existir dentro de un entorno empresarial.
 - Las organizaciones necesitan implementar todos estos 20 controles críticos para lograr el mejor entorno de seguridad y mantener el mismo para siempre. Si las empresas no pueden establecer 20, al menos pueden intentar establecer 10 controles de seguridad para llegar a la mitad.
- Framework NIST
 - El Instituto Nacional de Estándares y Tecnología (NIST) de los EE.UU. tiene políticas y normas similares que están documentadas y se dirigen a las organizaciones gubernamentales para desarrollar prácticas efectivas de seguridad de la información. También se puede aplicar a otras industrias. Hay Controlled Unclassified Information (CUI), que será el enfoque principal de este marco.
- PCI DSS
 - El Estándar Payment Card Industry Data Security Standard (PCI DSS) es un marco de ciberseguridad diseñado para mejorar la seguridad de las cuentas de pago, que protege las transacciones de débito, crédito y tarjetas de efectivo. Todos estos Frameworks se construyen y documentan para garantizar que las empresas cumplan con los estándares de la industria y mantengan su seguridad limpia y segura.

Implementación de Frameworks de Ciberseguridad

Después de identificar el Framework de Ciberseguridad adecuado para la empresa, esto debe practicarse según las directrices del documento. Para hacer eso, se deben implementar algunos pasos para que las cosas comiencen y se pongan en marcha.

- Las empresas primero necesitan probar e **identificar la postura de seguridad** actual dentro de su entorno
- **Analizar los proyectos existentes**, el proceso involucrado en estos proyectos y los recursos involucrados con ellos.
- ***Comprender el Framework de Ciberseguridad*** leyendo los documentos.
- **Distintuir qué controles** de seguridad existen y no existen dentro de la red empresarial
- **Comunique** dónde se están retrasando las capas de seguridad y **defina un plan** para establecer el mismo
- **Resalte los controles** que superan a los controles definidos por el Framework
- **Discuta todo el plan** con los actores clave, incluidos los interesados, y **continúe con la implementación**
- **Auditar el progreso** de la implementación continuamente.
- **Generar informes** y realizar reuniones para medir los desafíos.
- **Documentar todo el proceso** de auditorías y otros beneficios.

Los Framework de Ciberseguridad desempeñarán un papel clave en el establecimiento y mantenimiento de situaciones cibernéticas imprevistas, dando a las organizaciones una ventaja sobre los delincuentes cibernéticos.

Las empresas deben comprender las demandas que necesitan para mantenerse al día, analizar todos los procedimientos de implementación y hacer lo mismo solo después de discutir lo mismo con las partes interesadas y los departamentos de TI.

Ventajas y desventajas

Ventajas

- Los Framework de Ciberseguridad y sus políticas pueden superponerse entre sí, lo que permite a las organizaciones cumplir con múltiples marcos con el mínimo esfuerzo.
- Ciberseguridad mejorada.
- Mejor protección de datos
- Fácil cumplimiento y gestión de auditoría.

Desventajas

- La implementación puede llevar días, afectando la productividad.
- Una implementación incorrecta puede llevar a lagunas de seguridad
- Se pueden aplicar limitaciones financieras
- Con los ataques cibernéticos cada vez más sofisticados, las organizaciones deben seguir los marcos de seguridad cibernética adecuados y crear mejores defensas para mantener a los hackers a raya.
- El establecimiento de los Frameworks de Ciberseguridad puede llevarlo a la mitad del cumplimiento, pero mantener los mismos siempre producirá excelentes resultados para la ciberseguridad de su organización, manteniéndolos a la misma seguridad que a sus clientes.

1.5 Seguridad Operacional y Organizacional

1.5.1 Ingeniería Social

- La ingeniería social es el arte de explotar la psicología humana, en lugar de las técnicas de hacking, para acceder a edificios, sistemas o datos.
- Por ejemplo, en lugar de tratar de encontrar una vulnerabilidad de software, un ingeniero social podría llamar a un empleado y hacerse pasar por una persona de soporte de TI, tratando de engañar al empleado para que divulgue su contraseña.
- Incluso si tienes todas las ventajas y alertas cuando se trata de asegurar tu centro de datos, tus despliegues en la nube, la seguridad física de tu edificio, y has invertido en tecnologías defensivas, tienes las políticas y procesos de seguridad correctos y mides su eficacia y mejoras continuamente, todavía un ingeniero social astuto puede abrirse camino a través (o alrededor).



1.5.2 Políticas Organizacionales

- es una orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la organización, en ella se contemplan las normas y responsabilidades de cada área de la organización.
- Las políticas empresariales son guías para orientar la acción;
- son lineamientos generales a observar en la toma de decisiones, sobre algún problema que se repite una y otra vez dentro de una organización.
- las políticas son criterios generales de ejecución que complementan el logro de los objetivos y facilitan la implementación de las estrategias. Las políticas deben ser dictadas desde el nivel jerárquico más alto de la empresa.



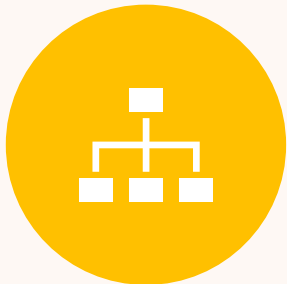
Metodología de implementación



Fase I: Diseño y desarrollo de la política, en la cual se contempla desde la necesidad, definición, hasta su redacción.



Fase II: Validación y aprobación de la política, se procede a realizar las revisiones y ajustes requeridos, para su posterior aprobación por parte de los involucrados.



Fase III: Divulgación a todos los niveles de la organización, consiste en formalizar a todos los miembros de la organización la vigencia y aplicación de la misma.



Fase IV: Mantenimiento de la política en cuanto a cumplimiento y vigencia, se refiere a los ajustes o actualizaciones que requiera dicho instrumento, se recomienda hacer revisiones y/o actualizaciones al menos una vez por año.

Beneficios de la aplicación de las políticas

Aseguran un trato equitativo para todos los empleados.

Generan seguridad de comunicación interna en todos los niveles.

Es fuente de conocimiento inicial, rápido y claro, para ubicar en su puesto nuevos empleados.

Facilita una comunicación abierta y promueve la honestidad.

Desarrolla la autoridad, poder y liderazgo.

Asegura la confianza, transparencia, objetividad y aprendizaje.

Son indispensables para una adecuada delegación de autoridad.

Reflejan la imagen de la empresa y deben reajustarse a tiempo.

Recomendaciones

1. Su redacción **debe ser sencilla y con lenguaje claro**, concreto y preciso, no deben existir ambigüedades.
 2. La política es parte esencial de la vida organizacional de una empresa, por lo cual **su letra no debe ser muerta (definir, aplicar y cumplir)**.
 3. **Debe ser adaptable a través del tiempo**, por lo cual entra en juego la fase de mantenimiento.
- **Normas**
 - Son reglas específicas que se deben seguir o a que se deben ajustar las conductas, tareas, o actividades en una organización para poder llevar a cabo el cumplimiento de una política organizacional. Cabe destacar que forman parte del contenido de las políticas organizacionales.

1.6 Continuidad de Negocio y DRM

Para empezar y haciendo analogía.....

- **Evento** es el síntoma de que podemos enfermar,
- **Incidente** es cuando la enfermedad es evidente pero tenemos medios para controlarla.
- **Desastre** es cuando tenemos que ir a urgencias.

Desastres.

Son Incidentes se nos escapan de las manos, no podemos resolverlos de forma inmediata o son muy repentinos, produciendo daños serios a nuestros sistemas de trabajo normal o a nuestras instalaciones.

llamamos incidentes de seguridad a los sucesos, de diferente naturaleza, que tienen consecuencias negativas para nuestros negocios:

- denegación de servicio
- acceso no autorizado
- espionaje y robo de información
- borrado o pérdida de información,
- etc.

Si queremos estar preparados....

En caso de sufrir este tipo de incidentes graves de seguridad, el primer paso será reconocerlos y poner los medios para gestionarlos.

En general, el departamento de informática será el encargado de ello, realizando las tareas de gestión de incidentes:

- Establecer **sistemas de recolección de eventos**
 - que nos permitan monitorizar las **alertas** de seguridad;
- **Analizar los incidentes de seguridad** que se hayan detectado,
 - documentarlos y catalogarlos estableciendo su prioridad;
- **estudiar los incidentes** que hayan tenido lugar analizando sus causas,
 - y así poder establecer medidas de seguridad adicionales que protejan nuestros activos de nuevos incidentes de índole similar;
- poner en marcha un **punto central de comunicación**,
 - para recibir y difundir información de incidentes de seguridad entre las partes correspondientes;
- establecer **procedimientos de respuesta** ante incidentes
 - y mantenerlos actualizados para saber qué pasos debemos dar y así poder gestionarlos correctamente.

Si gestionamos los incidentes, reconoceremos mejor aquellos que podrían hacer peligrar nuestra continuidad.

Para estar preparado en caso de que sucedan, debemos poner en marcha un **Plan de Recuperación ante Desastres** (DRP o Disaster Recovery Plan por sus siglas en inglés) dentro del Plan de Contingencia y Continuidad de Negocio.

1.6.1 Eventos de Desastre

- Un desastre es cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización.
 - Por ejemplo, la caída de un servidor como consecuencia de una subida de tensión o un ataque.

Las organizaciones deben estar preparadas ante cualquier tipo de desastre de manera que se reduzca el impacto que pueda ocasionar. Para ello, desarrollan planes de contingencia que permiten la prevención y recuperación de desastres informáticos.

1.6.2 Continuidad y Recuperación

- La continuidad del negocio describe los procesos y procedimientos puestos en marcha por una organización con el fin de garantizar que sus funciones esenciales puedan continuar tras producirse un incidente grave:
 - pérdida de información
 - inutilización o colapso del software
 - Inundación
 - Incendio
 - ataque terrorista
 - paralización de un planta por una avería técnica, etc.

1.6.2 Continuidad y Recuperación

La continuidad del negocio es la “capacidad estratégica y táctica de la organización para planificar y responder ante los incidentes e interrupciones del negocio con el fin de permitir la continuidad de las actividades operativas y comerciales en un nivel aceptable previamente definido”.

Recuperación ante desastres se refiere “al proceso, políticas y procedimientos relacionados con preparar la recuperación o continuación de la infraestructura tecnológica crítica de una organización después de un desastre natural o producido por el hombre”.

1.6.2 Continuidad y Recuperación

Como puede verse en las definiciones anteriores, en la recuperación ante desastres el énfasis se encuentra en la tecnología, mientras que para la continuidad del negocio son las actividades comerciales.

- Por lo tanto, la primera es parte de la segunda; la puede considerar como uno de los principales facilitadores de las actividades comerciales, o como la parte tecnológica de la continuidad del negocio.

1.6.2 Continuidad y Recuperación

- Una forma sencilla de acercar estos dos conceptos es:
 - ver la gestión de la continuidad como un proceso global de identificación y planificación para contrarrestar los riesgos de continuidad del negocio, y parte de dicha planificación debe incluir la recuperación del negocio desde un escenario de desastre para volver a la normalidad del trabajo.
 - La continuidad del negocio es principalmente un asunto comercial, no un tema exclusivo de TI. Si el departamento de TI implementara la continuidad del negocio para toda la organización, no podría definir la criticidad de las actividades comerciales ni de la información.
- Probablemente la mejor forma de organizar la implementación de la continuidad del negocio es que el sector comercial lidere el proyecto; de esta forma lograría mayor concientización y aceptación de todos los sectores de la organización. El departamento de TI debe cumplir su función en ese proyecto, una función clave, preparar los planes de recuperación ante desastres.

1.6.3 Evaluación de Impacto

- El objetivo es determinar qué impacto podría llegar a tener un desastre sobre las funciones críticas del negocio.
- Éste es básicamente un informe que nos muestra el costo ocasionado por la interrupción de los procesos de negocio. Una vez obtenido este informe, la compañía tiene la capacidad de clasificar los procesos de negocio en función de su criticidad y lo que es más importante: establecer la prioridad de recuperación (o su orden secuencial).
- En el BIA se identifican los componentes claves requeridos para continuar con las Operaciones de Negocio luego de un incidente,

1.6.3 Evaluación de Impacto

dentro de estos componentes se encuentran:

- Personal requerido
- Áreas de trabajo
- Registros vitales
- Aplicativos críticos
- Dependencias de otras áreas
- Dependencias de terceras partes
- Criticidad de los recursos de información
- Participación del personal de seguridad informática y los usuarios finales
- Análisis de todos los tipos de recursos de información

Tres aspectos claves para el análisis:

- Criticidad de los recursos de información relacionados con los procesos críticos del negocio
- Período de recuperación crítico antes de incurrir en pérdidas significativas
- Sistema de clasificación de riesgos

1.6.4 Backups

- Un respaldo es una copia de la información que una organización genera, utiliza y actualiza a lo largo del tiempo, también este término se emplea para referirse a las copias de seguridad que se llevan a cabo en:
 - Sistemas de información.
 - bases de datos.
 - Software de aplicación.
 - Sistemas operativos.
 - Documentos.
 - Utilerías.
 - Etc.

El objetivo de un respaldo, es garantizar la recuperación de la información, en caso que haya sido eliminada, dañada o alterada al presentarse alguna contingencia.

1.6.4 Backups

- Existe una regla denominada 3-2-1 aplicada sobre todo, para aquellos archivos de importancia crítica:
 - **3.- Mantener tres copias del archivo:** la original y dos respaldos. Esto disminuirá la probabilidad de perder información por tener unidades dañadas por malware o problema físico.
 - **2.- Guardar los archivos en dos unidades distintas** de almacenamiento a fin de protegerlos de diferentes daños (por ejemplo disco duro y memoria flash).
 - **1.- Mantener una de las copias “fuera de sitio”** (offsite), es decir, en un lugar físico distinto al lugar de trabajo (casa, taller, bodega, caja fuerte, etc.).

1.6.4 Backups

Tipos de copias de seguridad

- Completa.
 - Se realiza una copia de seguridad de todos los archivos y carpetas seleccionados. Cuando se ejecutan copias posteriores, nuevamente se hace una copia de seguridad de todo el listado de archivos. La restauración de una copia de seguridad completa es rápida. Sin embargo, cada ejecución es lenta y ocupa más espacio con respecto a las otras tipologías.
- Incremental.
 - Primero se realiza una copia de seguridad completa y las siguientes copias incluyen únicamente los cambios realizados desde la última copia de seguridad. Es mucho más rápida que una copia de seguridad completa y requiere menos espacio, pero la restauración es más lenta que con una copia de seguridad completa o diferencial.
- Diferencial.
 - Se realiza una copia de seguridad de todos los cambios realizados desde la última copia de seguridad completa. Es mucho más rápida y requiere menos espacio de almacenamiento que una copia de seguridad completa, pero más que una copia de seguridad incremental. Las restauraciones son más lentas que con una copia de seguridad completa, pero más rápidas que con copias de seguridad incrementales.

1.6.4 Backups

Tipos de copias de seguridad

- **Espejo.**
 - Es un reflejo fiel de la fuente que se está respaldando, lo que implica que un archivo eliminado en el origen, también se eliminará en la copia de seguridad. Debido a esto, este tipo de copia de seguridad debe usarse con precaución.
- **Sintética completa.**
 - Reconstruye la imagen de copia de seguridad completa usando todas las copias incrementales o diferenciales. Puede almacenarse en cintas en localizaciones externas, con la ventaja de que se reduce el tiempo de restauración.
- **Backup incremental inverso.**
 - Es una copia de seguridad incremental de los cambios realizados entre dos instancias de una copia espejo. Después de la copia completa inicial, cada copia sucesiva aplica los cambios a la anterior completa, creando una nueva copia de seguridad sintética completa cada vez, mientras se mantiene la capacidad de volver a las versiones anteriores
- **Protección de datos continua (CDP).**
 - Permite una mayor cantidad de puntos de restauración con respecto a los demás tipos de copia de seguridad

1.6.4 Backups

Tipos de copias de seguridad según su destino

Además, según el destino de la copias, podemos hablar de copias de seguridad:

- **Locales.**
 - cuando el medio de almacenamiento se mantiene a mano o en el mismo edificio que la fuente. Puede tratarse de discos duros o unidades de almacenamiento conectado en red (NAS).
- **Externas.**
 - cuando el medio de almacenamiento se mantienen en una ubicación geográfica diferente de la fuente (otra oficina, otro edificio o ubicaciones externas). De esta manera se consigue protección adicional contra robos, incendios, inundaciones y otros desastres naturales.
- **Remotas.**
 - cuando, además de ser externas, es posible acceder, restaurar o administrar las copias de seguridad sin estar físicamente presente en la instalación de almacenamiento de respaldo.
- **En línea.**
 - cuando se realizan en un medio de almacenamiento que siempre está conectado de forma segura a una red o conexión a Internet. Es un servicio ofrecido hoy en día por muchos centros de datos. Es también llamado copia de seguridad en la nube, si es proporcionado como un servicio cloud.

1.6.4 Backups

- copias de seguridad según nuestras necesidades
- Cada tipo de copia de seguridad funciona de manera diferente. En realidad, no siempre hay que elegir un tipo concreto, sino que es posible combinar distintos tipos de copias de seguridad para desarrollar una estrategia de protección de nuestros datos.
- Ejemplos de estrategias podrían ser:
 - 1.Una copia completa cada día.
 - 2.Una copia completa semanal y una diferencial diaria.
 - 3.Una copia completa semanal y una incremental diaria.