

**PROGRAMA DE ESTUDIO DE ARQUITECTURA DE PLATAFORMAS Y SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN**

**PLAN DE GESTIÓN DE RIESGOS Y CONTINGENCIA, APLICANDO LA METODOLOGÍA MAGERIT EN EL ISTRFA**

**INTEGRANTES**

Collantes Portilla Candy

Montalván Pintado Edilsa

Nanfuñay Carrión Javier

Neyra Quesquen Renzo

**Chiclayo, Julio del 2023**

**INDICE**

[INTRODUCCIÓN 1](#_heading=h.1fob9te)

[I.](#_heading=h.3znysh7) NOMBRE DEL PROYECTO: 2

[II.](#_heading=h.2et92p0) DEFINICIÓN DEL PROBLEMA O NECESIDAD DEL NEGOCIO 2

[III.](#_heading=h.tyjcwt) OBJETIVOS 3

[3.1.](#_heading=h.3dy6vkm) OBJETIVOS DEL NEGOCIO 3

[3.1.1.](#_heading=h.1t3h5sf) OBJETIVO GENERAL: 3

[3.1.2.](#_heading=h.4d34og8) OBJETIVOS ESPECÍFICOS: 3

[3.2.](#_heading=h.2s8eyo1) OBJETIVOS DEL PROYECTO 3

[3.2.1.](#_heading=h.17dp8vu) OBJETIVO GENERAL 3

[3.2.2.](#_heading=h.3rdcrjn) OBJETIVOS ESPECÍFICOS 4

[IV.](#_heading=h.26in1rg) ALINEAMIENTO CON PLAN ESTRATÉGICO DEL NEGOCIO 4

[V.](#_heading=h.lnxbz9) ETAPAS Y ACTIVIDADES CONTEMPLADAS EN EL PROYECTO 6

[VI.](#_heading=h.35nkun2) ALCANCE DEL PROYECTO 7

[VII.](#_heading=h.1ksv4uv) NORMAS Y REFERENCIAS 8

[7.1.](#_heading=h.44sinio) Disposiciones legales y normas aplicadas. 8

[7.2.](#_heading=h.2jxsxqh) Métodos, herramientas y prototipos 9

[7.2.1.](#_heading=h.z337ya) Métodos y herramientas: 9

[7.2.2.](#_heading=h.3j2qqm3) Modelos y recursos. 10

[Gestión de Incidentes 11](#_heading=h.1y810tw)

[3.1 Incidentes de seguridad 11](#_heading=h.4i7ojhp)

[3.2 Identificación y características 12](#_heading=h.2xcytpi)

[3.3 Sistema de detección de intrusos: mapeo de infraestructura TI 14](#_heading=h.1ci93xb)

[Respuesta ante incidentes de seguridad 14](#_heading=h.3whwml4)

[4.1 Definición de un plan de respuesta a incidentes 14](#_heading=h.2bn6wsx)

[4.2 Detección de un incidente de seguridad: Recolección de información 15](#_heading=h.qsh70q)

[4.3 MAPEO 16](#_heading=h.3as4poj)

[4.4 Contención, erradicación y recuperación 16](#_heading=h.1pxezwc)

[4.5 Identificación del atacante y posibles actuaciones legales 19](#_heading=h.49x2ik5)

[4.6 Documentación del Incidente de seguridad 22](#_heading=h.2p2csry)

[4.7 Análisis y revisión a posteriori del incidente: verificación de la intrusión 23](#_heading=h.147n2zr)

[4.8 Prácticas recomendadas 27](#_heading=h.3o7alnk)

[CONCLUSIONES: 28](#_heading=h.23ckvvd)

[RECOMENDACIONES: 29](#_heading=h.ihv636)

[BIBLIOGRAFIA: 30](#_heading=h.32hioqz)

[GLOSARIO DE TERMINOS: 30](#_heading=h.1hmsyys)

[ANEXOS 32](#_heading=h.41mghml)

# INTRODUCCIÓN

El Instituto Superior Tecnológico República Federal de Alemania (ISTRFA) se encuentra en constante búsqueda de mejoras en la gestión de la seguridad de la información y la protección de su infraestructura y sus activos. Con el fin de fortalecer su enfoque en la gestión de riesgos, se ha propuesto la implementación de un Plan de Gestión de Riesgos basado en la reconocida metodología MAGERIT.

Este proyecto tiene como objetivo principal desarrollar e implementar un plan integral que permita identificar, evaluar y gestionar los riesgos asociados a los procesos, sistemas y activos tecnológicos del ISTRFA. La metodología MAGERIT proporcionará un marco estructurado para llevar a cabo este proceso, garantizando una comprensión clara de los riesgos y su impacto potencial en el instituto.

A través de la aplicación de este plan, se espera lograr una gestión más efectiva de los riesgos, mejorando la capacidad de respuesta frente a posibles amenazas y minimizando los impactos negativos en las operaciones del ISTRFA. Además, se promoverá una cultura de seguridad sólida, involucrando a todo el personal y fomentando buenas prácticas en la gestión de riesgos.

El presente informe detallará los pasos a seguir, las etapas de implementación y los recursos necesarios para llevar a cabo este plan de gestión de riesgos en el ISTRFA. Se espera que los resultados obtenidos fortalezcan la seguridad y la confiabilidad de las operaciones, contribuyendo al logro de los objetivos estratégicos del instituto.

# NOMBRE DEL PROYECTO:

PLAN DE GESTIÓN DE RIESGOS Y CONTINGENCIA, APLICANDO LA METODOLOGÍA MAGERIT EN EL ISTRFA.

# DEFINICIÓN DEL PROBLEMA O NECESIDAD DEL NEGOCIO

El problema o necesidad del negocio que motiva la implementación de este plan de gestión de riesgos puede estar relacionado con la falta de un enfoque sistemático y estructurado para identificar, evaluar y gestionar los riesgos en el ámbito tecnológico y de seguridad de la información del instituto.

Algunos elementos específicos que podrían considerarse en la definición del problema o necesidad del negocio son:

1. Riesgos no identificados o subestimados: Puede haber una falta de conciencia o conocimiento sobre los riesgos potenciales asociados con los activos tecnológicos y los procesos del instituto. Esto podría llevar a una subestimación de los riesgos y, por lo tanto, a una falta de medidas preventivas y de respuesta adecuadas.

Por lo tanto, el proyecto permitirá identificar y evaluar los riesgos asociados a los activos de la institución, como sistemas de información, infraestructura de red, bases de datos y equipos. Al gestionar adecuadamente estos riesgos, se protegerá la integridad, disponibilidad y confidencialidad de los activos, evitando posibles pérdidas financieras, daños reputacionales y violaciones de la privacidad.

1. Brechas en la seguridad: Podría haber vulnerabilidades o deficiencias en los sistemas de seguridad existentes, lo que puede facilitar la explotación de amenazas y la ocurrencia de incidentes de seguridad. Esto podría poner en riesgo la integridad, disponibilidad y confidencialidad de los datos y activos del instituto.

La implementación de un plan de gestión de riesgos fomenta una cultura de seguridad dentro del instituto. Al involucrar a todo el personal en el proceso de identificación y mitigación de riesgos, promoviendo la conciencia y responsabilidad compartida en la protección de los activos y la información. Esto contribuye a la creación de un entorno seguro y confiable para estudiantes, personal y colaboradores del instituto.

1. Cumplimiento normativo insuficiente: El instituto puede estar enfrentando desafíos para cumplir con las regulaciones y normativas relevantes en materia de seguridad y protección de datos.

Realizar el presente proyecto ayudaría a alinear al Instituto con las regulaciones y normativas en materia de seguridad y protección de datos. Esto garantiza que el instituto cumpla con las obligaciones legales y normativas, evitando sanciones y posibles consecuencias legales.

# OBJETIVOS

## OBJETIVOS DEL NEGOCIO

### OBJETIVO GENERAL:

Fomentar la excelencia en la enseñanza, investigación y práctica académica para brindar una educación de calidad y formar profesionales altamente competentes en sus respectivas disciplinas

### OBJETIVOS ESPECÍFICOS:

* Establecer y fortalecer alianzas estratégicas con empresas, organizaciones y la comunidad local, para fomentar la transferencia de conocimientos, la colaboración en proyectos conjuntos y el apoyo mutuo en la formación de estudiantes y el desarrollo de proyectos de impacto social
* Promover la innovación, la investigación aplicada y el desarrollo tecnológico en áreas relevantes, fomentando la adopción de tecnologías emergentes y preparando a los estudiantes para enfrentar los desafíos del mundo laboral en constante evolución.
* Implementar procesos de aseguramiento de la calidad en todos los aspectos del funcionamiento del instituto, incluyendo la mejora continua de los programas académicos, la infraestructura, los servicios y la satisfacción de los estudiantes y demás partes interesadas.
* Promover la inclusión, la equidad y la diversidad en el acceso a la educación, garantizando que todos los estudiantes tengan igualdad de oportunidades para desarrollar su potencial académico y personal, sin importar su origen, género o cualquier otra característica personal.
* Fomentar la internacionalización de la institución a través de colaboraciones académicas, intercambios estudiantiles y programas de movilidad, para brindar a los estudiantes una perspectiva global y fortalecer la reputación del instituto a nivel internacional.

## OBJETIVOS DEL PROYECTO

### OBJETIVO GENERAL

Implementar un plan de gestión de riesgos utilizando la metodología MAGERIT en el ISTRFA, con el fin de proteger los activos tecnológicos, garantizar la continuidad de las actividades educativas y fortalecer la formación de profesionales altamente competentes en sus respectivas disciplinas.

### OBJETIVOS ESPECÍFICOS

* Identificar y analizar los activos tecnológicos críticos del instituto, incluyendo sistemas de información, infraestructura de red, bases de datos y otros recursos relevantes
* Realizar una evaluación exhaustiva de los riesgos asociados con cada uno de los activos identificados, considerando posibles amenazas, vulnerabilidades y el impacto que podrían tener en la integridad, disponibilidad y confidencialidad de la información
* Diseñar e implementar medidas preventivas para mitigarlos riesgos identificados, priorizando aquellos con mayor impacto y probabilidad de ocurrencia.
* Establecer un plan de respuesta ante incidentes que permita detectar, responder y recuperarse de manera efectiva ante posibles eventos de seguridad o interrupciones en los servicios tecnológicos.
* Capacitar al personal del instituto en temas de seguridad de la información y concientizar sobre las mejores prácticas para evitar incidentes de seguridad y proteger los activos tecnológicos.
* Establecer un proceso de revisión y mejora continua del plan de gestión de riesgos, asegurando que se adapte a los cambios tecnológicos, normativos y a las nuevas amenazas emergentes.
* Evaluar regularmente los resultados y beneficios del plan de gestión de riesgos, midiendo la efectividad de las acciones implementadas y su impacto en la reducción de riesgos y la protección de los activos del instituto.

# ALINEAMIENTO CON PLAN ESTRATÉGICO DEL NEGOCIO

Fomentar la excelencia en la enseñanza, investigación y práctica académica: Al proteger los activos tecnológicos y garantizar la continuidad de las actividades educativas, el proyecto contribuye a brindar una educación de calidad y formar profesionales altamente competentes en sus respectivas disciplinas.

Establecer y fortalecer alianzas estratégicas: Al identificar y gestionar los riesgos en el ámbito tecnológico y de seguridad de la información, el proyecto promueve la transferencia de conocimientos y la colaboración en proyectos conjuntos con empresas, organizaciones y la comunidad local. Esto fortalece las alianzas estratégicas y apoya la formación de estudiantes y el desarrollo de proyectos de impacto social.

Promover la innovación y el desarrollo tecnológico: Al mitigar los riesgos asociados a los activos tecnológicos, el proyecto fomenta la adopción de tecnologías emergentes y prepara a los estudiantes para enfrentar los desafíos del mundo laboral en constante evolución. Esto contribuye a la promoción de la innovación, la investigación aplicada y el desarrollo tecnológico en áreas relevantes.

Implementar procesos de aseguramiento de la calidad: Al identificar y gestionar los riesgos de manera efectiva, el proyecto busca implementar procesos de aseguramiento de la calidad en todos los aspectos del funcionamiento del instituto. Esto incluye la mejora continua de los programas académicos, la infraestructura, los servicios y la satisfacción de los estudiantes y demás partes interesadas.

Promover la inclusión, la equidad y la diversidad: Al proteger los activos tecnológicos y garantizar la seguridad de la información, el proyecto contribuye a crear un entorno seguro y confiable para todos los estudiantes, independientemente de su origen, género u otras características personales. Esto promueve la inclusión, la equidad y la diversidad en el acceso a la educación y brinda igualdad de oportunidades para desarrollar el potencial académico y personal de los estudiantes.

Fomentar la internacionalización: Al implementar un plan de gestión de riesgos y contingencia, el proyecto contribuye a fortalecer la reputación del instituto a nivel internacional. Esto se logra mediante colaboraciones académicas, intercambios estudiantiles y programas de movilidad, que brindan a los estudiantes una perspectiva global y promueven la internacionalización de la institución.

# ETAPAS Y ACTIVIDADES CONTEMPLADAS EN EL PROYECTO

| **Grupo** | | | **Organización de Recursos TI** | | | | | | | | | | | **2023** | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **N°** | **Actividades** | **Mayo** | | | | | **Junio** | | | | **Julio** | | | | |
| **Meses - Semanas** | **1** | | **2** | **3** | **4** | **1** | **2** | **3** | **4** | **1** | **2** | **3** | | **4** |
| **1** | **Determinar los activos** |  | |  | **x** | **x** | **x** | **x** | **x** |  |  |  |  | |  |
| **2** | **Determinar las amenazas** |  | |  |  |  | **x** | **x** | **x** | **x** |  |  |  | |  |
| **3** | **Determinar riesgos** |  | |  |  |  | **x** | **x** | **x** | **x** |  |  |  | |  |
| **4** | **Determinar salvaguardias** |  | |  |  |  |  |  |  | **x** | **x** | **x** | **x** | |  |
| **5** | **Determinar riesgo residual** |  | |  |  |  |  |  |  |  |  | **x** | **x** | | **x** |

# ALCANCE DEL PROYECTO

El proyecto tiene como objetivo principal implementar un Plan de Gestión de Riesgos basado en la metodología MAGERIT en el Instituto Superior Tecnológico República Federal de Alemania. El enfoque estará en identificar y mitigar los riesgos asociados a los activos tecnológicos críticos, con el fin de fortalecer la formación de profesionales competentes y garantizar la calidad educativa en el instituto.

**Entregables:**

a) Documento del Plan de Gestión de Riesgos: Un documento detallado que describa las estrategias, acciones y procedimientos para gestionar los riesgos tecnológicos en el instituto.

b) Evaluación de riesgos: Un informe que identifique y evalúe los riesgos asociados a los activos tecnológicos críticos.

c) Plan de respuesta ante incidentes: Un plan que defina las medidas y procedimientos para detectar, responder y recuperarse de posibles incidentes de seguridad.

d) Programa de capacitación en seguridad: Un programa de capacitación diseñado para promover una cultura de seguridad y conciencia de riesgos entre el personal y los estudiantes.

**Características de los entregables:**

Los entregables serán documentos escritos que estarán basados en la metodología MAGERIT. Serán claros, concisos y estarán estructurados de manera lógica, proporcionando detalles y orientación para la gestión de riesgos tecnológicos.

**Criterios de aceptación:**

a) Los entregables deben estar completos y cumplir con los requisitos establecidos en el alcance del proyecto.

b) Los entregables deben ser revisados y aprobados por el comité responsable de la gestión de riesgos del instituto.

c) Los entregables deben ser comprensibles y aplicables para el personal y los responsables de la gestión de riesgos del instituto.

**Restricciones:**

a) El proyecto estará limitado por el presupuesto asignado y los recursos disponibles para la implementación del plan.

b) El proyecto deberá completarse dentro de un marco de tiempo específico, considerando los plazos establecidos por la dirección del instituto.

**Supuestos:**

a) Se asume que se contarán con los recursos necesarios, incluyendo personal capacitado y acceso a información relevante para llevar a cabo la gestión de riesgos.

b) Se asume que el personal y los responsables involucrados en el proyecto estarán comprometidos y participarán activamente en la implementación del plan.

**Exclusiones:**

a) El proyecto no abarcará la gestión de riesgos no relacionados con los activos tecnológicos del instituto.

b) El proyecto no se encargará de la implementación directa de medidas de seguridad, sino que se centrará en el diseño y desarrollo del plan de gestión de riesgos.

# NORMAS Y REFERENCIAS

## Disposiciones legales y normas aplicadas.

**Normas y estándares:**

Norma Técnica Peruana ISO/IEC 27001: Norma que establece los requisitos para la gestión de seguridad de la información.

Norma Técnica Peruana ISO/IEC 31000: Norma que brinda directrices para la gestión de riesgos.

Norma Técnica Peruana ISO/IEC 27005: Norma que proporciona directrices para la gestión de riesgos de seguridad de la información.

MAGERIT: Metodología de análisis y gestión de riesgos de seguridad de la información desarrollada por el Ministerio de Hacienda y Administraciones Públicas de España, adaptada y aplicada en el contexto peruano.

**Legislación y regulaciones:**

Ley de Protección de Datos Personales: Legislación que establece los principios y requisitos para la protección de datos personales.

Ley Nº 29783, Ley de Seguridad y Salud en el Trabajo: Legislación que establece los lineamientos para la gestión de riesgos laborales.

Normativas sectoriales: Cualquier normativa específica relacionada con la gestión de riesgos y seguridad de la información en el sector educativo o tecnológico en Perú.

**Documentos internos del instituto:**

Políticas y procedimientos internos: Documentos establecidos por el Instituto Superior Tecnológico República Federal de Alemania que abordan la gestión de riesgos, seguridad de la información y protección de activos tecnológicos en el contexto peruano.

**Mejores prácticas y guías de referencia:**

Guías de la Autoridad de Protección de Datos Personales: Recursos proporcionados por la autoridad competente en materia de protección de datos personales.

Guías específicas de adaptación de MAGERIT para Perú: Recursos adicionales proporcionados por organizaciones o expertos peruanos que adapten la metodología MAGERIT al contexto peruano.

## Métodos, herramientas y prototipos

### Métodos y herramientas:

**Métodos:**

Determinación de activos: En esta etapa se establece el contexto del proyecto, se definen los objetivos y se identifican los activos de información relevantes.

Determinar amenazas: En esta etapa se identifican las amenazas y vulnerabilidades que podrían afectar los activos de información, se evalúa el impacto potencial y se determina la probabilidad de ocurrencia de los riesgos.

Determinación de riesgos: Se priorizan los riesgos identificados en función de su impacto y probabilidad, lo que permite establecer las acciones de mitigación más adecuadas.

Determinar salvaguardas: En esta etapa se desarrollan las estrategias y medidas de mitigación para reducir los riesgos identificados. Esto implica la implementación de controles de seguridad, la asignación de responsabilidades y la definición de planes de acción.

Determinar el riesgo residual: Se establecen mecanismos de monitoreo y revisión continua para garantizar que los controles implementados sean efectivos y se adapten a los cambios en el entorno tecnológico.

**Herramientas:**

Análisis FODA (Fortalezas, Oportunidades, Debilidades y Amenazas): Este modelo te ayudará a identificar y evaluar los factores internos y externos que pueden afectar el instituto. Analizar las fortalezas y debilidades internas te permitirá identificar los riesgos potenciales, mientras que identificar las oportunidades y amenazas externas te ayudará a anticipar posibles situaciones de riesgo.

Matriz de riesgos: Una matriz de riesgos es una herramienta visual que te permite identificar y clasificar los diferentes riesgos asociados con el funcionamiento del instituto. Puedes evaluar la probabilidad de ocurrencia de cada riesgo y su impacto potencial en el instituto. Esto te permitirá priorizar los riesgos y asignar recursos de manera adecuada para su mitigación.

Análisis de causas y efectos: Utilizando técnicas como el diagrama de Ishikawa (también conocido como "espina de pescado" o "diagrama de causa y efecto"), podrás identificar las posibles causas de los riesgos y comprender mejor sus efectos potenciales en el instituto. Esto te ayudará a diseñar estrategias de mitigación más efectivas.

Herramientas de gestión de riesgos: Para la gestión efectiva de los riesgos identificados, se emplearán herramientas que permitan documentar, monitorear y controlar las acciones tomadas. Estas herramientas facilitarán el seguimiento de las medidas de mitigación implementadas, así como la actualización continua de la información relacionada con los riesgos.

### Modelos y recursos.

**Análisis FODA:**

Entrevistas o encuestas a personal docente, administrativo y estudiantes para identificar fortalezas, debilidades, oportunidades y amenazas.

Revisión de informes internos y externos sobre el rendimiento académico, la satisfacción de los estudiantes, la competencia en el mercado, etc.

Análisis de datos demográficos y tendencias educativas para identificar oportunidades y amenazas a largo plazo.

**Matriz de riesgos:**

Plantillas de matriz de riesgos que te permitan clasificar los riesgos según su probabilidad e impacto.

Sesiones de trabajo con equipos multidisciplinarios para identificar y evaluar los riesgos.

Información histórica sobre incidentes previos y problemas recurrentes en el instituto.

**Análisis de causas y efectos:**

Técnicas de lluvia de ideas (brainstorming) para identificar posibles causas de los riesgos.

Diagramas de Ishikawa o diagramas de causa y efecto para visualizar las causas potenciales de los riesgos.

Entrevistas o grupos de enfoque con personas clave para obtener información sobre las posibles causas y efectos.

**Planificación de contingencias:**

Plantillas de planes de contingencia que te guíen en la identificación de acciones y recursos necesarios.

Recursos financieros asignados para hacer frente a situaciones de emergencia.

Lista de contactos de proveedores, personal de emergencia y otros recursos externos relevantes.

# Gestión de Incidentes

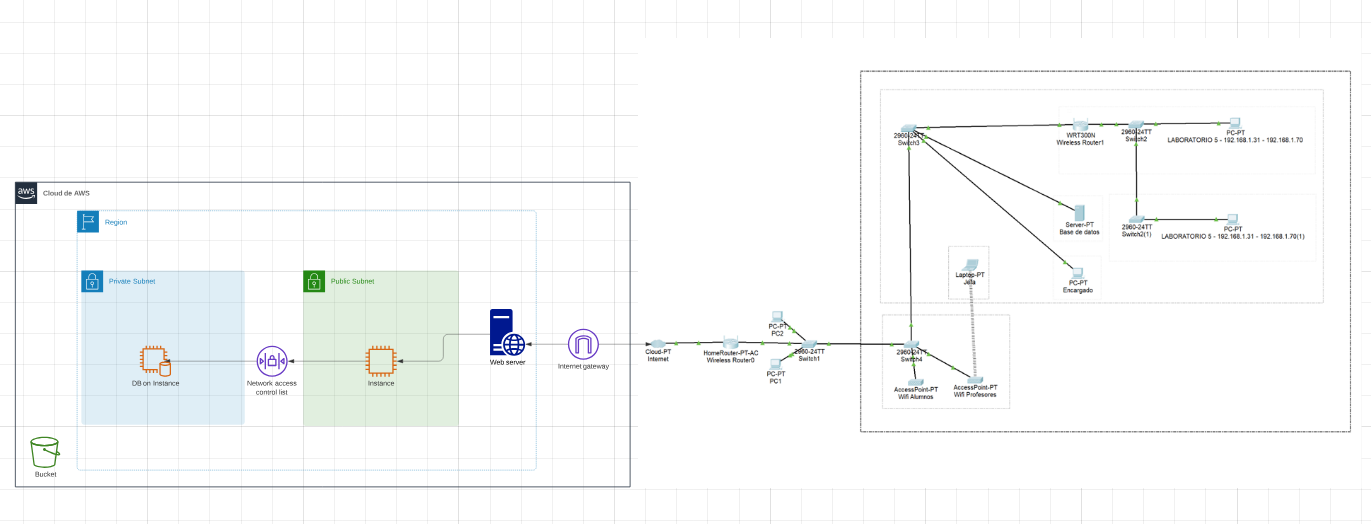
## 3.1 Incidentes de seguridad

1. Ataque de fuerza bruta: Intentos repetitivos y sistemáticos de adivinar contraseñas o claves de acceso mediante la prueba de múltiples combinaciones hasta encontrar la correcta.
2. Ataque de inyección de código: Inserción de código malicioso en aplicaciones o sistemas a través de entradas no validadas, lo que puede permitir a los atacantes ejecutar comandos o acceder a datos sensibles.
3. Ataque de intercepción de datos: Obtención no autorizada de datos mientras se transmiten entre sistemas o dispositivos, generalmente mediante el uso de técnicas de escucha o manipulación de tráfico de red.
4. Ataque de denegación de servicio distribuido (DDoS): Un ataque en el que múltiples sistemas comprometidos se utilizan para inundar un sistema o red objetivo con tráfico, lo que resulta en una interrupción del servicio.
5. Escalamiento de privilegios: Obtención no autorizada de privilegios administrativos o de usuario avanzados para acceder a recursos o realizar acciones restringidas.
6. Exposición de datos sensibles: Divulgación accidental o intencionada de información confidencial
7. Vulnerabilidades de software: Identificación de fallas de seguridad en el código o diseño del software, que podrían ser explotadas por atacantes para acceder o comprometer el sistema.
8. Errores de programación: Problemas en el desarrollo de software que pueden causar comportamientos inesperados, como bloqueos, fugas de memoria o exposición de datos sensibles.
9. Actualizaciones de software fallidas: Problemas durante la instalación o actualización de software, lo que podría generar conflictos o dejar el sistema en un estado inestable o vulnerable.
10. Robo o pérdida de hardware: Extravío o sustracción de dispositivos de hardware, como computadoras portátiles, servidores o dispositivos móviles, lo que podría resultar en la exposición de datos confidenciales o el acceso no autorizado a la infraestructura.
11. Fallos de suministro de energía: Interrupciones en la electricidad o problemas con el suministro de energía que pueden provocar la caída del sistema y la pérdida de datos.
12. Problemas de conectividad de red: Dificultades para establecer o mantener una conexión de red estable, lo que puede afectar la disponibilidad y el rendimiento de los sistemas y servicios.
13. Robo o divulgación de datos sensibles: Acceso no autorizado a bases de datos o archivos que contienen información confidencial, como datos personales, contraseñas o datos financieros.
14. Ransomware: Infección de sistemas con malware que cifra archivos y exige un rescate para su recuperación.
15. Interferencia con la integridad del software: Manipulación maliciosa del código o configuración del software para alterar su funcionamiento normal o introducir comportamientos no deseados.

## 3.2 Identificación y características

* Ataque de fuerza bruta:
  + Características: Intentos repetitivos y sistemáticos de adivinar contraseñas o claves de acceso mediante la prueba de múltiples combinaciones hasta encontrar la correcta.
  + Ejemplo: Un atacante realiza un gran número de intentos de inicio de sesión utilizando diferentes combinaciones de contraseñas para obtener acceso no autorizado.
* Ataque de inyección de código:
  + Características: Inserción de código malicioso en aplicaciones o sistemas a través de entradas no validadas, lo que puede permitir a los atacantes ejecutar comandos o acceder a datos sensibles.
  + Ejemplo: Un atacante explota una vulnerabilidad en un formulario web para insertar código malicioso que se ejecuta en el servidor y permite el acceso no autorizado a datos.
* Ataque de intercepción de datos:
  + Características: Obtención no autorizada de datos mientras se transmiten entre sistemas o dispositivos, generalmente mediante el uso de técnicas de escucha o manipulación de tráfico de red.
  + Ejemplo: Un atacante utiliza un programa de captura de paquetes para interceptar y leer información confidencial, como contraseñas, que se transmite a través de una red no segura.
* Ataque de denegación de servicio distribuido (DDoS):
  + Características: Un ataque en el que múltiples sistemas comprometidos se utilizan para inundar un sistema o red objetivo con tráfico, lo que resulta en una interrupción del servicio.
  + Ejemplo: Un atacante utiliza una botnet para enviar una gran cantidad de solicitudes de conexión a un servidor web, sobrecargándolo y dejándolo inaccesible para los usuarios legítimos.
* Escalamiento de privilegios:
  + Características: Obtención no autorizada de privilegios administrativos o de usuario avanzados para acceder a recursos o realizar acciones restringidas.
  + Ejemplo: Un atacante aprovecha una vulnerabilidad en un sistema para elevar sus privilegios y obtener acceso a funciones o datos a los que normalmente no debería tener acceso.
* Exposición de datos sensibles:
  + Características: Divulgación accidental o intencionada de información confidencial.
  + Ejemplo: Una base de datos mal configurada expone información personal de los usuarios, como nombres, direcciones y números de seguridad social, en línea y sin protección.
* Incidente de vulnerabilidades de software:
  + Características: Identificación de fallas de seguridad en el código o diseño del software, que podrían ser explotadas por atacantes para acceder o comprometer el sistema.
  + Ejemplo: Se descubre una vulnerabilidad en un sistema de gestión de contenido que permite a un atacante obtener acceso no autorizado a la base de datos.
* Incidente de errores de programación:
  + Características: Problemas en el desarrollo de software que pueden causar comportamientos inesperados, como bloqueos, fugas de memoria o exposición de datos sensibles.
  + Ejemplo: Un error de programación en una aplicación financiera resulta en la pérdida de datos o en cálculos incorrectos.
* Incidente de actualizaciones de software fallidas:
  + Características: Problemas durante la instalación o actualización de software, lo que podría generar conflictos o dejar el sistema en un estado inestable o vulnerable.
  + Ejemplo: Después de una actualización de software, los sistemas se vuelven inestables y experimentan bloqueos frecuentes.
* Incidente de robo o pérdida de hardware:
  + Características: Extravío o sustracción de dispositivos de hardware, como computadoras portátiles, servidores o dispositivos móviles, lo que podría resultar en la exposición de datos confidenciales o el acceso no autorizado a la infraestructura.
  + Ejemplo: Un servidor es robado de un centro de datos, lo que permite a los atacantes acceder a datos confidenciales almacenados en él.
* Incidente de fallos de suministro de energía:
  + Características: Interrupciones en la electricidad o problemas con el suministro de energía que pueden provocar la caída del sistema y la pérdida de datos.
  + Ejemplo: Un corte de energía repentino causa la pérdida de datos en los servidores y afecta la disponibilidad de los servicios en el instituto.
* Incidente de problemas de conectividad de red:
  + Características: Dificultades para establecer o mantener una conexión de red estable, lo que puede afectar la disponibilidad y el rendimiento de los sistemas y servicios.
  + Ejemplo: Una falla en el enrutador principal provoca una interrupción en la conectividad de red, lo que impide el acceso a los servicios en línea del instituto.
* Incidente de robo o divulgación de datos sensibles:
  + Características: Acceso no autorizado a bases de datos o archivos que contienen información confidencial, como datos personales, contraseñas o datos financieros.
  + Ejemplo: Un atacante obtiene acceso a una base de datos de estudiantes y divulga la información personal de los estudiantes en línea.
* Incidente de ransomware:
  + Características: Infección de sistemas con malware que cifra archivos y exige un rescate para su recuperación.
  + Ejemplo: Los sistemas del instituto son infectados por un ransomware que encripta archivos críticos y exige un pago para su desencriptación.
* Incidente de interferencia con la integridad del software:
  + Características: Manipulación maliciosa del código o configuración del software para alterar su funcionamiento normal o introducir comportamientos no deseados.
  + Ejemplo: Un atacante modifica el código fuente de una aplicación de pago en línea para desviar los pagos a su propia cuenta.

## 3.3 Sistema de detección de intrusos: mapeo de infraestructura TI



# Respuesta ante incidentes de seguridad

## 4.1 Definición de un plan de respuesta a incidentes

Un plan de respuesta a incidentes es un conjunto de procedimientos y acciones predefinidas que se establecen para abordar de manera eficiente y efectiva los incidentes de seguridad que puedan ocurrir en una organización. El objetivo principal del plan es minimizar el impacto de los incidentes, mitigar las consecuencias y restaurar rápidamente la normalidad en los sistemas y operaciones.

El plan de respuesta a incidentes define roles y responsabilidades claras para los miembros del equipo de respuesta, establece los pasos a seguir para detectar, reportar, evaluar y responder a los incidentes, así como los métodos y herramientas que se utilizarán. También incluye la comunicación interna y externa, la notificación a las partes interesadas relevantes y los procedimientos para documentar y analizar los incidentes.

Algunos elementos comunes que se pueden encontrar en un plan de respuesta a incidentes son:

* Equipo de respuesta a incidentes: Definición de los roles y responsabilidades de los miembros del equipo y sus contactos de referencia.
* Procedimientos de detección y reporte: Establecimiento de mecanismos para la detección temprana de incidentes y los canales de comunicación interna para reportarlos.
* Evaluación y clasificación de incidentes: Definición de criterios para evaluar la gravedad y el impacto de los incidentes, así como su clasificación en función de la naturaleza y la severidad.
* Respuesta y mitigación: Descripción de las acciones y medidas que se deben tomar para contener y mitigar los incidentes, incluyendo la preservación de evidencia, la restauración de sistemas y la implementación de controles de seguridad adicionales.
* Comunicación y notificación: Establecimiento de los canales de comunicación interna y externa para informar a los miembros del equipo, la dirección de la organización, las autoridades pertinentes y otras partes interesadas sobre los incidentes y las medidas tomadas.
* Análisis y aprendizaje: Definición de los procedimientos para realizar una investigación posterior al incidente, analizar las causas raíz y las lecciones aprendidas, y aplicar medidas correctivas y preventivas para evitar futuros incidentes similares.

## 4.2 Detección de un incidente de seguridad: Recolección de información

Mediante el método de observación se ha podido identificar los siguientes incidentes:

* Ataque de fuerza bruta:
  + Un atacante realiza un gran número de intentos de inicio de sesión utilizando diferentes combinaciones de contraseñas para obtener acceso no autorizado.
* Ataque de inyección de código:
  + Un atacante explota una vulnerabilidad en un formulario web para insertar código malicioso que se ejecuta en el servidor y permite el acceso no autorizado a datos.
* Ataque de intercepción de datos:
  + Un atacante utiliza un programa de captura de paquetes para interceptar y leer información confidencial, como contraseñas, que se transmite a través de una red no segura.
* Ataque de denegación de servicio distribuido (DDoS):
  + Un atacante utiliza una botnet para enviar una gran cantidad de solicitudes de conexión a un servidor web, sobrecargándolo y dejándolo inaccesible para los usuarios legítimos.
* Escalamiento de privilegios:
  + Un atacante aprovecha una vulnerabilidad en un sistema para elevar sus privilegios y obtener acceso a funciones o datos a los que normalmente no debería tener acceso.
* Exposición de datos sensibles:
  + Una base de datos mal configurada expone información personal de los usuarios, como nombres, direcciones y números de seguridad social, en línea y sin protección.
* Incidente de vulnerabilidades de software:
  + Se descubre una vulnerabilidad en un sistema de gestión de contenido que permite a un atacante obtener acceso no autorizado a la base de datos.
* Incidente de errores de programación:
  + Un error de programación en una aplicación financiera resulta en la pérdida de datos o en cálculos incorrectos.
* Incidente de actualizaciones de software fallidas:
  + Después de una actualización de software, los sistemas se vuelven inestables y experimentan bloqueos frecuentes.
* Incidente de robo o pérdida de hardware:
  + Un servidor es robado de un centro de datos, lo que permite a los atacantes acceder a datos confidenciales almacenados en él.
* Incidente de fallos de suministro de energía:
  + Un corte de energía repentino causa la pérdida de datos en los servidores y afecta la disponibilidad de los servicios en el instituto.
* Incidente de problemas de conectividad de red:
  + Una falla en el enrutador principal provoca una interrupción en la conectividad de red, lo que impide el acceso a los servicios en línea del instituto.
* Incidente de robo o divulgación de datos sensibles:
  + Un atacante obtiene acceso a una base de datos de estudiantes y divulga la información personal de los estudiantes en línea.
* Incidente de ransomware:
  + Los sistemas del instituto son infectados por un ransomware que encripta archivos críticos y exige un pago para su desencriptación.
* Incidente de interferencia con la integridad del software:
  + Un atacante modifica el código fuente de una aplicación de pago en línea para desviar los pagos a su propia cuenta.

## 4.3 MAPEO

## 4.4 Contención, erradicación y recuperación

* Incidente de ataque de fuerza bruta:

Contención: Bloquear o limitar los intentos de inicio de sesión fallidos, por ejemplo, mediante el bloqueo de cuentas después de un número determinado de intentos fallidos.

Erradicación: Identificar la fuente del ataque y tomar medidas para bloquearla o mitigarla, como bloquear direcciones IP sospechosas o implementar sistemas de detección de intrusos.

Recuperación: Revisar las políticas y prácticas de contraseñas, fortalecer la autenticación y educar a los usuarios sobre la importancia de utilizar contraseñas seguras.

* Incidente de ataque de inyección de código:

Contención: Validar y filtrar todas las entradas de usuario para evitar la ejecución de código malicioso.

Erradicación: Identificar y corregir las vulnerabilidades en las aplicaciones o sistemas afectados que permitieron la inyección de código.

Recuperación: Realizar pruebas exhaustivas de seguridad y auditorías de código para prevenir futuros ataques de inyección de código.

* Incidente de ataque de intercepción de datos:

Contención: Utilizar protocolos de cifrado, como SSL/TLS, para proteger la transmisión de datos sensibles.

Erradicación: Identificar las vulnerabilidades en la red o en los sistemas que permitieron la intercepción de datos y corregirlas.

Recuperación: Notificar a los usuarios afectados, tomar medidas para garantizar la integridad de los datos comprometidos y mejorar la seguridad de la red.

* Incidente de ataque de denegación de servicio distribuido (DDoS):

Contención: Implementar soluciones de mitigación de DDoS, como firewalls de aplicaciones web y servicios de protección contra DDoS, para filtrar el tráfico malicioso y mantener la disponibilidad del servicio.

Erradicación: Identificar y bloquear las fuentes del ataque, como las direcciones IP de los bots utilizados en el ataque.

Recuperación: Restablecer la disponibilidad del servicio, revisar las defensas contra DDoS y desarrollar planes de contingencia para futuros ataques.

* Incidente de escalamiento de privilegios:

Contención: Restringir los privilegios de acceso para usuarios y cuentas, implementar políticas de control de acceso y monitorear los cambios en los niveles de privilegios.

Erradicación: Identificar y corregir las vulnerabilidades en los sistemas que permitieron el escalamiento de privilegios.

Recuperación: Revisar y reforzar las políticas de seguridad y acceso, así como proporcionar capacitación y concientización sobre la importancia de proteger los privilegios de acceso.

* Incidente de exposición de datos sensibles:

Contención: Restringir el acceso a los datos sensibles, implementar cifrado de datos y establecer políticas de control de acceso.

Erradicación: Identificar y corregir las vulnerabilidades en los sistemas o bases de datos que permitieron la exposición de datos.

Recuperación: Notificar a los afectados, implementar medidas de protección adicional, como monitoreo de crédito, y mejorar la seguridad de los sistemas para prevenir futuras exposiciones de datos.

* Incidente de vulnerabilidades de software:

Contención: Parchear y actualizar regularmente el software con las últimas correcciones de seguridad.

Erradicación: Realizar análisis de vulnerabilidades y pruebas de seguridad para identificar y corregir las vulnerabilidades en el software utilizado.

Recuperación: Implementar un proceso de gestión de vulnerabilidades continuo, realizar pruebas de seguridad periódicas y mantenerse actualizado sobre las últimas amenazas y parches de seguridad.

* Incidente de errores de programación:

Contención: Realizar pruebas exhaustivas de calidad de software y asegurarse de que se sigan buenas prácticas de desarrollo.

Erradicación: Identificar y corregir los errores de programación en el código para evitar comportamientos inesperados o vulnerabilidades.

Recuperación: Establecer procesos de revisión de código y asegurar que se realicen pruebas de calidad rigurosas antes de implementar nuevas versiones del software.

* Incidente de actualizaciones de software fallidas:

Contención: Realizar copias de seguridad regulares antes de aplicar actualizaciones y asegurarse de tener un plan de contingencia en caso de fallas en las actualizaciones.

Erradicación: Identificar y corregir las causas de las fallas en las actualizaciones, como incompatibilidades o errores en el proceso de actualización.

Recuperación: Restaurar desde las copias de seguridad, solucionar los problemas de las actualizaciones y mejorar los procesos de actualización para evitar futuras fallas.

* Incidente de robo o pérdida de hardware:

Contención: Informar de inmediato la pérdida o robo del hardware a las autoridades correspondientes y bloquear o desactivar los dispositivos para prevenir el acceso no autorizado.

Erradicación: Realizar un seguimiento y búsqueda exhaustivos del hardware perdido o robado, y tomar medidas para prevenir futuros incidentes, como implementar sistemas de seguimiento de activos.

Recuperación: Restaurar los datos y la funcionalidad perdidos a través de copias de seguridad y reemplazar los dispositivos robados o perdidos con nuevos, asegurándose de implementar medidas de seguridad adecuadas.

* Incidente de fallos de suministro de energía:

Contención: Implementar fuentes de alimentación alternativas, como generadores de respaldo o baterías UPS, para garantizar la continuidad del suministro de energía durante interrupciones.

Erradicación: Identificar las causas de los fallos de suministro de energía y tomar medidas correctivas, como reparaciones o mejoras en la infraestructura eléctrica.

Recuperación: Restaurar el suministro de energía y asegurarse de que los sistemas y equipos afectados vuelvan a funcionar correctamente.

* Incidente de problemas de conectividad de red:

Contención: Realizar pruebas de conectividad y monitorear el rendimiento de la red para identificar y solucionar problemas de conectividad de forma rápida.

Erradicación: Identificar las causas subyacentes de los problemas de conectividad y tomar medidas correctivas, como configuraciones incorrectas o fallas en los dispositivos de red.

Recuperación: Restaurar la conectividad de red y asegurarse de que los sistemas y servicios afectados estén funcionando correctamente.

* Incidente de robo o divulgación de datos sensibles:

Contención: Aislar el sistema o red afectada para evitar que el ransomware se propague y comunicarse con las autoridades correspondientes.

Erradicación: Identificar y eliminar el ransomware del sistema o red afectada y restablecer los archivos y datos cifrados a través de copias de seguridad.

Recuperación: Mejorar la seguridad del sistema para prevenir futuros ataques de ransomware, como mantener el software actualizado y educar al personal sobre las prácticas de seguridad.

* Incidente de interferencia con la integridad del software:

Contención: Identificar y aislar el software afectado para evitar que la interferencia maliciosa se propague y cause más daño.

Erradicación: Restaurar la integridad del software eliminando cualquier código malicioso o manipulación, y fortalecer las medidas de seguridad para prevenir futuras interferencias.

Recuperación: Restaurar el funcionamiento normal del software y garantizar que se realicen pruebas de seguridad rigurosas para detectar y prevenir futuras interferencias.

## 4.5 Identificación del atacante y posibles actuaciones legales

* IDENTIFICACION DEL ATACANTE:

Ataque de fuerza bruta: Este tipo de ataque puede ser llevado a cabo por estudiantes, profesores, usuarios internos o incluso usuarios externos que intenten adivinar contraseñas o claves de acceso para obtener acceso no autorizado a sistemas o recursos protegidos.

Ataque de inyección de código: Este tipo de ataque generalmente requiere un conocimiento técnico más avanzado, por lo que es más probable que sea llevado a cabo por usuarios internos o externos con habilidades en programación y seguridad. Los estudiantes o profesores con conocimientos avanzados podrían intentar este tipo de ataque para explotar vulnerabilidades en aplicaciones o sistemas de la institución.

Ataque de intercepción de datos: Este tipo de ataque puede ser realizado por usuarios internos o externos con conocimientos en redes y seguridad. Pueden intentar interceptar datos confidenciales mientras se transmiten entre sistemas o dispositivos, aprovechando vulnerabilidades en la configuración de red o utilizando técnicas de escucha o manipulación de tráfico de red.

Ataque de denegación de servicio distribuido (DDoS): Este tipo de ataque generalmente es llevado a cabo por usuarios externos, a menudo utilizando una red de dispositivos comprometidos (botnet). Estos atacantes pueden intentar inundar la red o los sistemas de la institución con un tráfico masivo para saturar los recursos y causar una interrupción del servicio.

Escalamiento de privilegios: Este tipo de ataque puede ser realizado por usuarios internos o externos que hayan obtenido un nivel de acceso inicial a los sistemas de la institución. Buscan elevar sus privilegios para obtener acceso a recursos o realizar acciones restringidas que normalmente no estarían disponibles para ellos.

Exposición de datos sensibles: Este incidente puede ser el resultado de una acción no intencional, como un error de programación o una mala configuración por parte de usuarios internos. También puede ser resultado de un ataque deliberado realizado por usuarios internos o externos con el objetivo de acceder y divulgar información confidencial.

Incidente de vulnerabilidades de software: Este tipo de incidente puede estar relacionado con errores de programación, actualizaciones de software fallidas o falta de medidas de seguridad adecuadas. Los errores de programación y las vulnerabilidades en el software pueden ser introducidos tanto por usuarios internos como externos durante el desarrollo o implementación de sistemas.

Incidente de errores de programación: Este incidente generalmente está relacionado con el trabajo de desarrollo de software realizado por estudiantes, profesores u otros usuarios internos. Los errores de programación pueden introducir vulnerabilidades y comportamientos inesperados en el software, lo que puede ser aprovechado por atacantes para obtener acceso no autorizado o causar interrupciones.

Incidente de actualizaciones de software fallidas: Este incidente puede estar relacionado con la implementación incorrecta de actualizaciones de software por parte de usuarios internos responsables de la administración de sistemas. Las actualizaciones fallidas pueden dejar el sistema en un estado inestable o vulnerable, lo que puede ser aprovechado por atacantes para acceder o comprometer los sistemas.

Incidente de robo o pérdida de hardware: Este incidente puede ser el resultado de un descuido o robo de dispositivos de hardware por parte de estudiantes, profesores u otros usuarios internos. El robo o pérdida de hardware puede llevar a la exposición de datos confidenciales o el acceso no autorizado a la infraestructura.

Incidente de fallos de suministro de energía: Este incidente generalmente está fuera del control de los atacantes internos, pero puede ser resultado de eventos fortuitos o fallas en la infraestructura eléctrica. Sin embargo, usuarios internos malintencionados podrían realizar acciones para interrumpir el suministro de energía, pero esto sería altamente inusual.

Incidente de problemas de conectividad de red: Este incidente puede ser causado por problemas técnicos, fallas en la configuración o ataques deliberados en la red. Los problemas de conectividad de red pueden afectar la disponibilidad y el rendimiento de los sistemas y servicios de la institución.

Incidente de robo o divulgación de datos sensibles: Este incidente puede ser resultado de un robo o una divulgación intencional de datos confidenciales por parte de usuarios internos o externos. Los usuarios internos con acceso a información sensible puedenaprovechar su posición privilegiada para robar o divulgar datos. Los usuarios externos pueden intentar infiltrarse en los sistemas de la institución para acceder y robar datos sensibles.

Incidente de ransomware: Este tipo de incidente generalmente es llevado a cabo por usuarios externos que infectan los sistemas de la institución con malware de ransomware. El objetivo es cifrar los archivos y exigir un rescate para su recuperación. Los usuarios internos podrían involuntariamente desencadenar un ataque de ransomware al hacer clic en enlaces o descargar archivos maliciosos.

Incidente de interferencia con la integridad del software: Este incidente puede ser causado por usuarios internos o externos que manipulan maliciosamente el código o la configuración del software para alterar su funcionamiento normal o introducir comportamientos no deseados. Esto puede llevar a fallos en el software o comprometer la seguridad de los sistemas.

* ACTUACIONES LEGALES:

Ataque de fuerza bruta: Este tipo de ataque puede ser sancionado en Perú según los artículos 6 y 7 de la Ley de Delitos Informáticos, que establecen penas de privación de libertad para quienes accedan a sistemas informáticos sin autorización.

Ataque de inyección de código: En Perú, este tipo de ataque podría ser considerado un delito informático y sancionado en función de los daños ocasionados. La Ley de Delitos Informáticos contempla penas para quienes produzcan, introduzcan o propaguen códigos maliciosos, como virus informáticos.

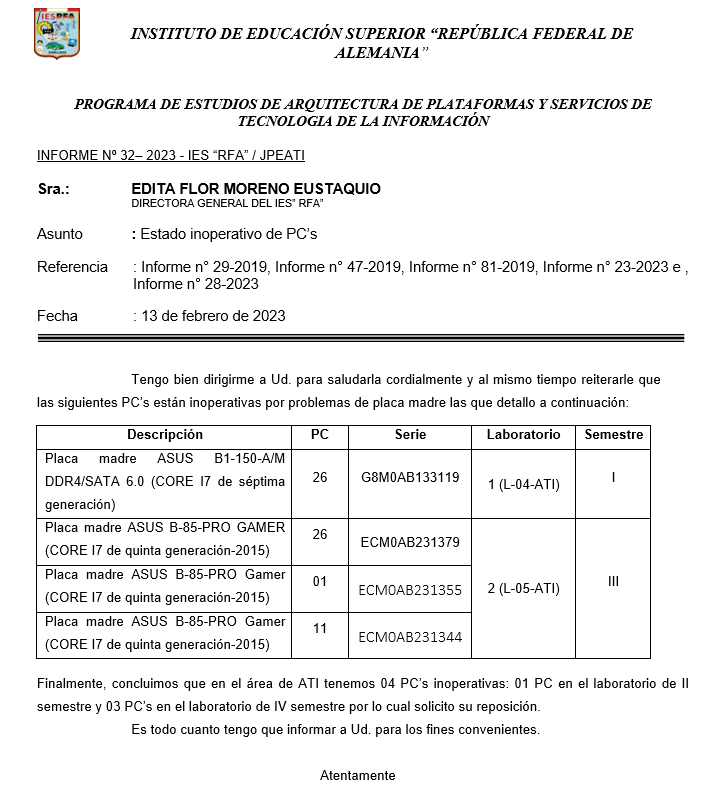
Ataque de intercepción de datos: La interceptación no autorizada de datos está penalizada en Perú según el artículo 9 de la Ley de Delitos Informáticos, que establece penas para aquellos que intercepten ilegalmente comunicaciones electrónicas o accedan a datos personales sin autorización.

Ataque de denegación de servicio distribuido (DDoS): En Perú, los ataques DDoS pueden ser considerados delitos informáticos según el artículo 12 de la Ley de Delitos Informáticos, que establece penas para quienes interrumpan o dificulten el funcionamiento de sistemas informáticos sin autorización.

Escalamiento de privilegios: El acceso no autorizado a recursos o privilegios puede ser considerado un delito informático en Perú y penalizado según los artículos 6 y 7 de la Ley de Delitos Informáticos.

Exposición de datos sensibles: La divulgación no autorizada de datos personales o sensibles podría ser sancionada en Perú según la Ley de Protección de Datos Personales (Ley N° 29733), que establece medidas de protección y sanciones en caso de incumplimiento.

## 4.6 Documentación del Incidente de seguridad



## 4.7 Análisis y revisión a posteriori del incidente: verificación de la intrusión

**ATAQUE DE FUERZA BRUTA:**

Descripción: Intentos repetitivos y sistemáticos de adivinar contraseñas o claves de acceso mediante la prueba de múltiples combinaciones hasta encontrar la correcta.

Análisis y revisión:

* Recopilar registros de actividad relacionados con los intentos de inicio de sesión y los patrones de intentos fallidos.
* Analizar los registros para identificar las direcciones IP, nombres de usuario y patrones de intentos de fuerza bruta.
* Determinar si se ha logrado una intrusión exitosa y, de ser así, qué acciones se llevaron a cabo una vez obtenido el acceso.
* Identificar las vulnerabilidades o debilidades que permitieron el ataque de fuerza bruta, como contraseñas débiles o políticas de bloqueo de cuentas ineficientes.
* Recomendar mejoras en la seguridad, como el uso de contraseñas más fuertes, implementación de bloqueos temporales después de múltiples intentos fallidos, y autenticación multifactorial.

**ATAQUE DE INYECCIÓN DE CÓDIGO:**

Descripción: Inserción de código malicioso en aplicaciones o sistemas a través de entradas no validadas, lo que puede permitir a los atacantes ejecutar comandos o acceder a datos sensibles.

Análisis y revisión:

* Analizar el código fuente de la aplicación o sistema afectado en busca de vulnerabilidades de inyección de código, como SQL injection o XSS (Cross-Site Scripting).
* Identificar las entradas no validadas que permitieron la inyección de código malicioso.
* Determinar el alcance del impacto y las acciones realizadas por los atacantes una vez que se ejecutó el código malicioso.
* Evaluar las medidas de seguridad existentes, como la validación de entrada y la desinfección de datos, para identificar las mejoras necesarias.
* Recomendar prácticas seguras de desarrollo de software, como el uso de consultas parametrizadas y la codificación segura, para prevenir futuros ataques de inyección de código.

**ATAQUE DE INTERCEPCIÓN DE DATOS:**

Descripción: Obtención no autorizada de datos mientras se transmiten entre sistemas o dispositivos, generalmente mediante el uso de técnicas de escucha o manipulación de tráfico de red.

Análisis y revisión:

* Revisar los registros de actividad de la red en busca de anomalías, como cambios en el volumen o patrones de tráfico.
* Identificar cualquier evidencia de intercepción de datos, como paquetes de red capturados o manipulados.
* Analizar las técnicas utilizadas por los atacantes para interceptar el tráfico de red, como el uso de sniffers o ataques man-in-the-middle (hombre en el medio).
* Evaluar las medidas de seguridad de red existentes, como el cifrado de datos y el uso de VPN (red privada virtual), para determinar si hubo alguna falla en su implementación.
* Recomendar mejoras en la seguridad de red, como el monitoreo continuo del tráfico de red, la implementación de cifrado de extremo a extremo y la educación sobre seguridad en el uso de redes públicas.

**ATAQUE DE DENEGACIÓN DE SERVICIO DISTRIBUIDO (DDOS):**

Descripción: Un ataque en el que múltiples sistemas comprometidos se utilizan para inundar un sistema o red objetivo con tráfico, lo que resulta en una interrupción del servicio.

Análisis y revisión:

* Analizar los registros de tráfico de red para identificar patrones anormales o picos repentinos en el volumen de tráfico.
* Identificar las direcciones IP o los sistemas involucrados en el ataque de denegación de servicio distribuido.
* Determinar el tipo de ataque DDoS utilizado, como ataques de inundación de tráfico o ataques de agotamiento de recursos.
* Evaluar las medidas de mitigación de DDoS existentes, como firewalls o sistemas de detección de intrusiones (IDS), para determinar si hubo alguna falla en su capacidad de respuesta.
* Recomendar mejoras en la infraestructura de red, como la implementación de servicios de mitigación de DDoS basados en la nube o el equilibrio de carga, para prevenir futuros ataques de denegación de servicio.

**ESCALAMIENTO DE PRIVILEGIOS:**

Descripción: Obtención no autorizada de privilegios administrativos o de usuario avanzados para acceder a recursos o realizar acciones restringidas.

Análisis y revisión:

* Investigar cómo se obtuvieron los privilegios adicionales o la escalada de privilegios por parte de los atacantes.
* Analizar los registros de actividad del sistema para identificar cualquier comportamiento inusual o cambios en los permisos de usuario.
* Determinar si hubo algún fallo en la configuración de los controles de acceso o en la gestión de usuarios y privilegios.
* Evaluar las políticas y procedimientos de gestión de privilegios existentes para identificar áreas de mejora, como la revisión regular de los permisos y la implementación de políticas de menor privilegio.
* Recomendar la implementación de soluciones de gestión de privilegios, como sistemas de gestión de identidad y acceso (IAM) o controles de acceso basados en roles (RBAC), para prevenir futuros casos de escalado de privilegios.

**EXPOSICIÓN DE DATOS SENSIBLES:**

Descripción: Divulgación accidental o intencionada de información confidencial.

Análisis y revisión:

* Identificar el origen de la exposición de datos sensibles, como una configuración incorrecta de los permisos de archivo o una brecha de seguridad.
* Evaluar el alcance de la exposición de datos y los posibles impactos para los individuos o la organización.
* Analizar las políticas y controles de seguridad existentes, como el cifrado de datos y la segmentación de redes, para identificar posibles debilidades o brechas.
* Recomendar mejoras en la protección de datos, como la implementación de medidas adicionales de control de acceso, el uso de cifrado y la capacitación en seguridad de la información para los empleados.
* Identificar las medidas de respuesta y notificación adecuadas, como el cumplimiento de las leyes y regulaciones de protección de datos y la notificación a las partes afectadas según corresponda.

**VULNERABILIDADES DE SOFTWARE:**

Descripción: Identificación de fallas de seguridad en el código o diseño del software, que podrían ser explotadas por atacantes para acceder o comprometer el sistema.

Análisis y revisión:

* Analizar el código y diseño del software afectado para identificar las vulnerabilidades de seguridad presentes.
* Utilizar herramientas de escaneo de vulnerabilidades y pruebas de penetración para identificar y explotar las vulnerabilidades.
* Evaluar el impacto de las vulnerabilidades y determinar si se ha llevado a cabo algún acceso no autorizado o compromiso del sistema.
* Recomendar acciones correctivas, como la aplicación de parches de seguridad, la revisión del código y el fortalecimiento de las medidas de seguridad en el ciclo de desarrollo de software.
* Establecer procedimientos para la revisión regular de las vulnerabilidades de software y la implementación de medidas proactivas para abordarlas.

**ERRORES DE PROGRAMACIÓN:**

Descripción: Problemas en el desarrollo de software que pueden causar comportamientos inesperados, como bloqueos, fugas de memoria o exposición de datos sensibles.

Análisis y revisión:

* Analizar el código fuente del software afectado para identificar los errores de programación y las áreas problemáticas.
* Realizar pruebas exhaustivas para reproducir los errores y comprender su impacto en el funcionamiento del software.
* Evaluar los posibles riesgos asociados con los errores, como la pérdida de datos o la exposición de información confidencial.
* Recomendar correcciones y mejoras en el código, como la implementación de controles de validación de entrada y la gestión adecuada de memoria.
* Establecer mejores prácticas de desarrollo de software, como la revisión de código, las pruebas de calidad y la capacitación en seguridad para los desarrolladores.

**ACTUALIZACIONES DE SOFTWARE FALLIDAS:**

Descripción: Problemas durante la instalación o actualización de software, lo que podría generar conflictos o dejar el sistema en un estado inestable o vulnerable.

Análisis y revisión:

* Investigar los problemas y errores encontrados durante la instalación o actualización del software.
* Evaluar las configuraciones y procedimientos utilizados durante la actualización para identificar posibles errores o fallos en el proceso.
* Determinar el impacto en la disponibilidad, integridad y seguridad del sistema debido a la actualización fallida.
* Recomendar mejores prácticas para la gestión de actualizaciones, como la realización de pruebas previas a la implementación, la realización de copias de seguridad adecuadas y la planificación de contingencias en caso de problemas.
* Establecer un proceso de revisión y aprobación adecuado para las actualizaciones de software en el futuro, con el fin de minimizar los riesgos asociados.

**ROBO O PÉRDIDA DE HARDWARE:**

Descripción: Extravío o sustracción de dispositivos de hardware, como computadoras portátiles, servidores o dispositivos móviles, lo que podría resultar en la exposición de datos confidenciales o el acceso no autorizado a la infraestructura.

Análisis y revisión:

* Investigar y documentar los detalles del incidente, incluyendo la ubicación, fecha y hora de la pérdida o robo de hardware.
* Evaluar el impacto potencial del incidente en términos de datos y acceso a la infraestructura.
* Revisar los procedimientos de seguridad existentes, como el cifrado de datos, la autenticación de dos factores y las políticas de almacenamiento seguro, para determinar si hubo alguna falla en su implementación.
* Recomendar acciones correctivas, como el reporte a las autoridades pertinentes, el cambio de contraseñas y credenciales, y la implementación de medidas adicionales de seguridad física.
* Establecer políticas y procedimientos claros para el manejo y almacenamiento seguro de dispositivos de hardware, así como para la notificación y respuesta en caso de pérdida o robo.

**FALLOS DE SUMINISTRO DE ENERGÍA:**

Descripción: Interrupciones en la electricidad o problemas con el suministro de energía que pueden provocar la caída del sistema y la pérdida de datos.

Análisis y revisión:

* Investigar y documentar los detalles de los fallos de suministro de energía, incluyendo la duración, frecuencia y ubicación.
* Evaluar el impacto del incidente en los sistemas y servicios afectados, incluyendo la pérdida de datos y el tiempo de inactividad.
* Revisar las medidas de respaldo de energía existentes, como los sistemas UPS (Uninterruptible Power Supply) y los generadores de respaldo, para determinar si hubo alguna falla en su funcionamiento.
* Recomendar mejoras en la infraestructura de energía, como la implementación de sistemas de respaldo más robustos y la realización de pruebas regulares de contingencia.
* Establecer procedimientos de respuesta y recuperación en caso de fallos de suministro de energía, incluyendo la priorización de servicios críticos y la realización de copias de seguridad regulares.

**PROBLEMAS DE CONECTIVIDAD DE RED:**

Descripción: Dificultades para establecer o mantener una conexión de red estable, lo que puede afectar la disponibilidad y el rendimiento de los sistemas y servicios.

Análisis y revisión:

* Investigar y documentar los problemas de conectividad de red, incluyendo la ubicación, duración y frecuencia de los incidentes.
* Evaluar el impacto del incidente en la disponibilidad y el rendimiento de los sistemas y servicios afectados.
* Revisar la infraestructura de red existente, incluyendo los dispositivos de red, los enlaces de comunicación y los proveedores de servicios, para identificar posibles puntos de falla.
* Recomendar mejoras en la infraestructura de red, como la implementación de redundancia de enlaces, la configuración adecuada de los dispositivos de red y la monitorización proactiva de la conectividad.
* Establecer procedimientos de respuesta y recuperación en caso de problemas de conectividad de red, incluyendo la notificación temprana a los proveedores de servicios y la implementación de medidas alternativas de comunicación.

**ROBO O DIVULGACIÓN DE DATOS SENSIBLES:**

Descripción: Acceso no autorizado a bases de datos o archivos que contienen información confidencial, como datos personales, contraseñas o datos financieros.

Análisis y revisión:

* Identificar cómo se llevó a cabo el robo o la divulgación de datos sensibles, como una brecha de seguridad en el sistema o la explotación de vulnerabilidades.
* Evaluar el alcance y el impacto de la violación de datos, incluyendo el tipo de información expuesta y el número de registros comprometidos.
* Revisar las medidas de seguridad existentes, como el cifrado de datos, el control de acceso y la monitorización de actividades sospechosas, para identificar posibles debilidades.
* Recomendar mejoras en la seguridad de datos, como la implementación de medidas adicionales de protección de datos, la educación sobre seguridad en el manejo de información confidencial y la realización de pruebas regulares de seguridad.
* Establecer un plan de respuesta a incidentes de seguridad, incluyendo la notificación a las partes afectadas, la cooperación con las autoridades competentes y la implementación de medidas correctivas para prevenir futuras brechas.

**RANSOMWARE:**

Descripción: Infección de sistemas con malware que cifra archivos y exige un rescate para su recuperación.

Análisis y revisión:

* Investigar cómo se produjo la infección de ransomware, como a través de correos electrónicos de phishing, descargas de archivos infectados o vulnerabilidades de seguridad explotadas.
* Evaluar el impacto de la infección de ransomware en los sistemas y los datos afectados, incluyendo la cantidad de archivos cifrados y las interrupciones del servicio.
* Revisar las medidas de seguridad existentes, como el software antivirus, los firewalls y las políticas de seguridad, para identificar posibles brechas en la defensa contra el ransomware.
* Recomendar mejoras en la seguridad, como la concienciación y capacitación en seguridad cibernética para los empleados, la implementación de sistemas de respaldo y recuperación de datos y la actualización regular de software y sistemas operativos.
* Establecer un plan de respuesta a incidentes de ransomware, incluyendo el aislamiento y la eliminación del malware, la restauración de archivos a partir de copias de seguridad y la cooperación con las autoridades pertinentes.

**INTERFERENCIA CON LA INTEGRIDAD DEL SOFTWARE:**

Descripción: Manipulación maliciosa del código o configuración del software para alterar su funcionamiento normal o introducir comportamientos no deseados.

Análisis y revisión:

* Identificar cómo se produjo la interferencia con la integridad del software, como la explotación de vulnerabilidades de seguridad o la manipulación de configuraciones.
* Evaluar el impacto de la interferencia en el funcionamiento del software, incluyendo las consecuencias para los datos, la disponibilidad y la confidencialidad.
* Revisar los controles de seguridad y las medidas de protección existentes, como la autenticación de software y la firma digital, para identificar posibles debilidades.
* Recomendar mejoras en la seguridad del software, como la implementación de mecanismos de control de integridad y autenticación de software, y la realización de pruebas de seguridad regulares.
* Establecer políticas y procedimientos para la gestión de cambios de software, incluyendo revisiones y aprobaciones, para prevenir la interferencia maliciosa en el futuro.

## 4.8 Prácticas recomendadas

* Mantener un enfoque de defensa en capas: Implementar múltiples capas de seguridad, como firewalls, sistemas de detección de intrusiones, sistemas de prevención de intrusiones, soluciones antivirus y antimalware, para proporcionar una protección más sólida contra diferentes tipos de amenazas.
* Actualizar y parchear regularmente: Mantener todos los sistemas y software actualizados con los últimos parches de seguridad para corregir vulnerabilidades conocidas y prevenir ataques basados en exploits conocidos.
* Fortalecer las contraseñas y utilizar autenticación multifactorial: Implementar políticas de contraseñas fuertes y únicas para todos los usuarios y considerar el uso de la autenticación multifactorial para agregar una capa adicional de seguridad.
* Realizar copias de seguridad regulares: Realizar copias de seguridad periódicas de los datos y sistemas críticos y almacenar las copias de seguridad en un lugar seguro fuera del sitio. También es importante realizar pruebas periódicas de restauración para garantizar la integridad de las copias de seguridad.
* Educación y concienciación sobre seguridad: Capacitar y educar regularmente a los empleados sobre las mejores prácticas de seguridad, incluyendo la identificación de correos electrónicos de phishing, la seguridad de contraseñas, el uso seguro de dispositivos y la protección de información confidencial.
* Implementar controles de acceso y políticas de privilegios mínimos: Limitar los privilegios de usuario y proporcionar solo los permisos necesarios para realizar tareas específicas. Implementar controles de acceso basados en roles para garantizar que cada usuario tenga los privilegios adecuados.
* Monitorear y analizar registros de actividad: Establecer una solución de gestión de registros y realizar un seguimiento de los registros de actividad para identificar actividades sospechosas o inusuales que podrían indicar un ataque en curso.
* Realizar pruebas de seguridad regulares: Realizar pruebas de penetración, escaneos de vulnerabilidades y auditorías de seguridad de forma regular para identificar posibles brechas o vulnerabilidades en los sistemas y aplicaciones.
* Implementar una respuesta a incidentes y un plan de recuperación de desastres: Tener en marcha un plan de respuesta a incidentes que establezca los pasos a seguir en caso de un incidente de seguridad y un plan de recuperación de desastres que permita restaurar los sistemas y servicios rápidamente.
* Realizar análisis y revisión a posteriori de incidentes: Después de cualquier incidente de seguridad, realizar un análisis y revisión exhaustiva para comprender las causas raíz, las lecciones aprendidas y las acciones correctivas necesarias para fortalecer la seguridad en el futuro.

# CONCLUSIONES:

* La seguridad de la información es un aspecto crítico en cualquier organización, y los incidentes de seguridad pueden ser provocados por diversas amenazas y vulnerabilidades.
* Los ataques de fuerza bruta, inyección de código y denegación de servicio distribuido (DDoS) son ejemplos comunes de incidentes de seguridad que pueden afectar la disponibilidad, integridad y confidencialidad de los sistemas y datos de una institución.
* La detección temprana de incidentes de seguridad es fundamental para una respuesta rápida y efectiva. Un sistema de detección de intrusos (IDS) bien implementado puede ayudar a identificar actividades sospechosas y mitigar los ataques.
* La gestión de vulnerabilidades de software y errores de programación es esencial para prevenir incidentes de seguridad. Las organizaciones deben realizar pruebas de seguridad periódicas, mantener el software actualizado y seguir buenas prácticas de desarrollo para reducir las posibilidades de explotación de vulnerabilidades.
* Los incidentes de robo o pérdida de hardware y fallos de suministro de energía pueden afectar la disponibilidad de los servicios y la integridad de los datos. Es importante implementar medidas de seguridad física y contar con planes de contingencia para hacer frente a estas situaciones.
* La comunicación y notificación adecuadas son fundamentales para coordinar las acciones de respuesta y minimizar el impacto de los incidentes. Es necesario establecer canales de comunicación interna y externa para informar a todas las partes interesadas relevantes.
* En el caso de incidentes relacionados con el robo, divulgación o exposición de datos sensibles, las organizaciones deben cumplir con las leyes y regulaciones de protección de datos y notificar a los afectados según corresponda.
* Para cada tipo de incidente, es esencial contar con un plan de respuesta a incidentes predefinido que defina roles y responsabilidades, procedimientos de detección y reporte, acciones de contención, erradicación y recuperación, así como medidas de análisis y aprendizaje para mejorar la seguridad en el futuro.
* La cooperación entre equipos de seguridad, personal técnico y la dirección de la organización es crucial para una respuesta efectiva y exitosa ante los incidentes de seguridad.

# RECOMENDACIONES:

* Implementar autenticación sólida: Utiliza métodos de autenticación multifactor (MFA) para agregar una capa adicional de seguridad. Esto ayudará a proteger las cuentas de usuario de accesos no autorizados.
* Mantener el software actualizado: Asegúrate de que todos los sistemas, aplicaciones y dispositivos estén actualizados con los últimos parches y actualizaciones de seguridad. Las vulnerabilidades conocidas a menudo son corregidas en las actualizaciones.
* Realizar evaluaciones periódicas de seguridad: Lleva a cabo pruebas de penetración y evaluaciones de seguridad de manera regular. Esto ayudará a identificar posibles vulnerabilidades y brechas de seguridad antes de que sean aprovechadas por los atacantes.
* Capacitar al personal en seguridad: Concientiza al personal sobre las prácticas de seguridad y los riesgos asociados con el manejo inadecuado de la información. Un personal informado será una línea de defensa más sólida contra ataques de ingeniería social.
* Establecer políticas de seguridad claras: Implementa políticas de seguridad bien definidas para el acceso a sistemas, manejo de datos y uso de dispositivos. Asegúrate de que todos los empleados las conozcan y cumplan.
* Implementar cifrado: Utiliza cifrado para proteger la información confidencial tanto en reposo como en tránsito. El cifrado ayuda a proteger los datos incluso si son interceptados por terceros.
* Respaldar regularmente los datos: Realiza copias de seguridad periódicas y asegúrate de que los datos críticos estén respaldados de forma segura. En caso de un incidente, esto permitirá la recuperación de la información perdida.
* Establecer controles de acceso: Limita los privilegios de acceso a la información y sistemas solo a los usuarios autorizados que necesiten dichos permisos para sus funciones.
* Monitorear y analizar registros de actividad: Configura sistemas de monitoreo de seguridad y registra las actividades del sistema para detectar posibles comportamientos anómalos o intentos de acceso no autorizados.
* Tener un plan de respuesta a incidentes: Desarrolla un plan de respuesta a incidentes detallado que defina las acciones a seguir en caso de un ataque o violación de seguridad. Practica simulacros de incidentes para asegurar que el personal esté preparado para responder adecuadamente.
* Evaluar la seguridad de proveedores y terceros: Si compartes información con proveedores externos, asegúrate de que también tengan buenas prácticas de seguridad y protección de datos.
* Cumplir con las regulaciones y normativas de seguridad: Asegúrate de cumplir con todas las leyes y regulaciones pertinentes relacionadas con la seguridad de la información y la privacidad de los datos.

# BIBLIOGRAFIA:

* <https://lucid.app/lucidchart/b87b28ec-b5b3-48bf-9192-8d147a66e8cc/edit?invitationId=inv_ea7c452b-e739-4c30-bb0e-e1dc4add9a61&page=0_0#>
* <https://repositorio.ulima.edu.pe/bitstream/handle/20.500.12724/3143/Loayza_Uyehara_Alexander.pdf?sequence=1>
* <https://www.mineducacion.gov.co/1759/articles-322548_Manual__Gestion_de_Incidentes_de_Seguridad_de_la_Informacion_e_Informatica_.pdf>
* <https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/1114/BC-TES-5892.pdf?sequence=1&isAllowed=y>
* **Metodología de la Investigación. 3ra Edición. Colombia,** Jan 2010, César Bernal, Bernal, César. (2010). Metodología de la Investigación. 3ra Edición. Colombia. Pearson. ISBN 978-958-699-128-5

# GLOSARIO DE TERMINOS:

* Firewall: Es una barrera de seguridad que controla y filtra el tráfico de red entre redes, como Internet y una red interna, con el fin de bloquear accesos no autorizados y proteger los sistemas de posibles amenazas externas.
* Malware: Es un término general que hace referencia a todo tipo de software malicioso diseñado para dañar, acceder de forma no autorizada o comprometer la seguridad de un sistema. Ejemplos incluyen virus, gusanos, troyanos y ransomware.
* Ransomware: Es un tipo de malware que restringe el acceso a un sistema o cifra los archivos del usuario y luego exige el pago de un rescate (ransom) para restaurar el acceso o descifrar los datos.
* Zero-day (Exploit): Es una vulnerabilidad de seguridad en un software o sistema que es desconocida por el fabricante o el público en general. Un ataque de día cero (zero-day attack) ocurre cuando un ciberdelincuente aprovecha esa vulnerabilidad antes de que se desarrolle un parche o solución.
* Detección de intrusiones (IDS): Es un sistema que monitorea el tráfico de red o actividad del sistema en busca de actividades maliciosas o no autorizadas y alerta o responde ante posibles incidentes de seguridad.
* Prevención de intrusiones (IPS): Es un sistema que, además de detectar intrusos o actividades maliciosas, toma medidas para bloquear o prevenir esos ataques en tiempo real.
* Phishing: Es un tipo de ataque de ingeniería social en el que los atacantes se hacen pasar por entidades legítimas, como empresas o instituciones conocidas, para obtener información confidencial de las víctimas, como contraseñas o detalles de tarjetas de crédito.
* Token de seguridad: Es un dispositivo físico o virtual que genera códigos temporales utilizados en la autenticación de dos factores (2FA) para mejorar la seguridad de las cuentas en línea.
* Hacking ético: También conocido como "pentesting ético", es el proceso de simular ataques de ciberseguridad en sistemas, redes o aplicaciones con el permiso del propietario para identificar vulnerabilidades y mejorar la seguridad.
* Biometría: Es un método de autenticación que utiliza características físicas o de comportamiento únicas, como huellas dactilares, reconocimiento facial o escaneo de iris, para verificar la identidad de una persona.
* Encriptación de extremo a extremo: Es un método de cifrado que protege la confidencialidad de los datos durante toda su transmisión, desde el emisor hasta el receptor, evitando que terceros no autorizados accedan a la información.
* Gestión de accesos: Es un conjunto de políticas y tecnologías que regulan y limitan los permisos de los usuarios para acceder a recursos y sistemas en una red o aplicación, garantizando que solo tengan acceso a la información relevante para su función o rol.
* Suplantación de identidad (Spoofing): Es una técnica utilizada para ocultar la verdadera identidad de un atacante al hacerse pasar por otra entidad o dirección de origen en línea.

# ANEXOS

* ENCUESTA

