SEGURIDAD INFORMÁTICA

JOSÉ PABLO HERNÁNDEZ

SEGURIDAD INFORMÁTICA

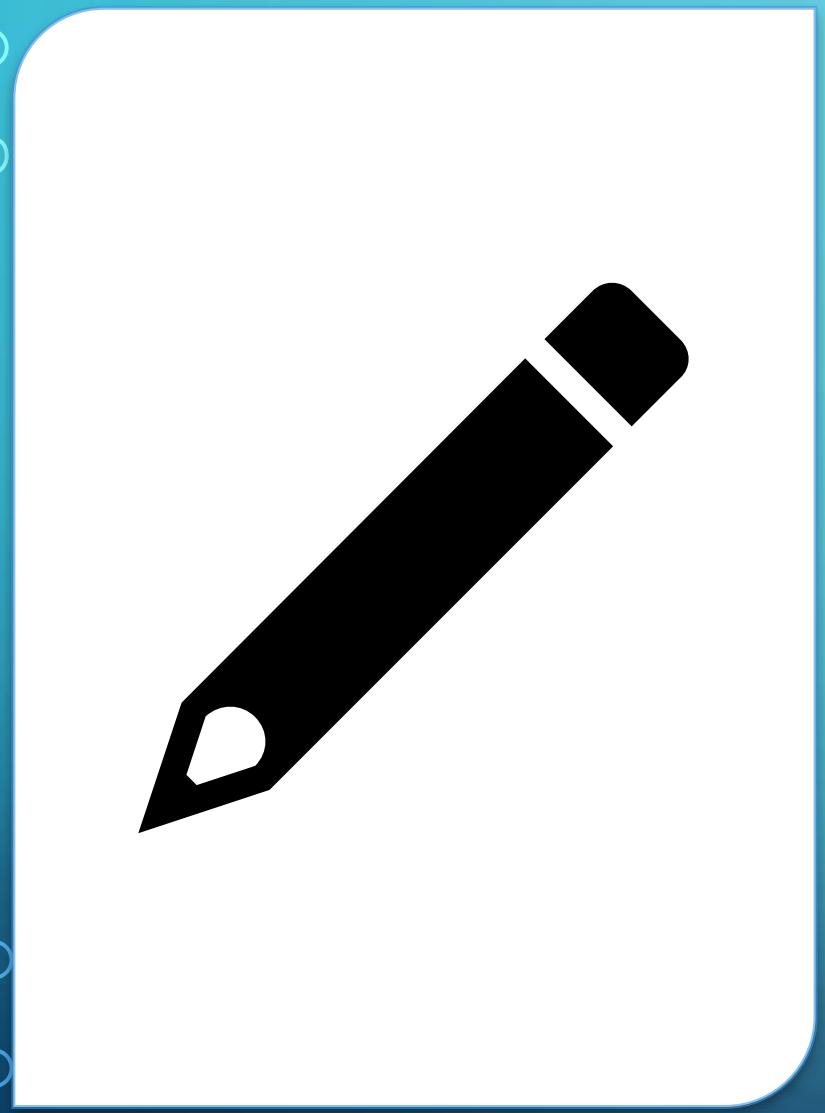
3.2.2.MF0488_3. Capítulo 2
Parte 2

Proceso de notificación y gestión de intentos de intrusión

JOSÉ PABLO HERNÁNDEZ

6. GUÍA PARA LA CLASIFICACIÓN Y ANÁLISIS INICIAL

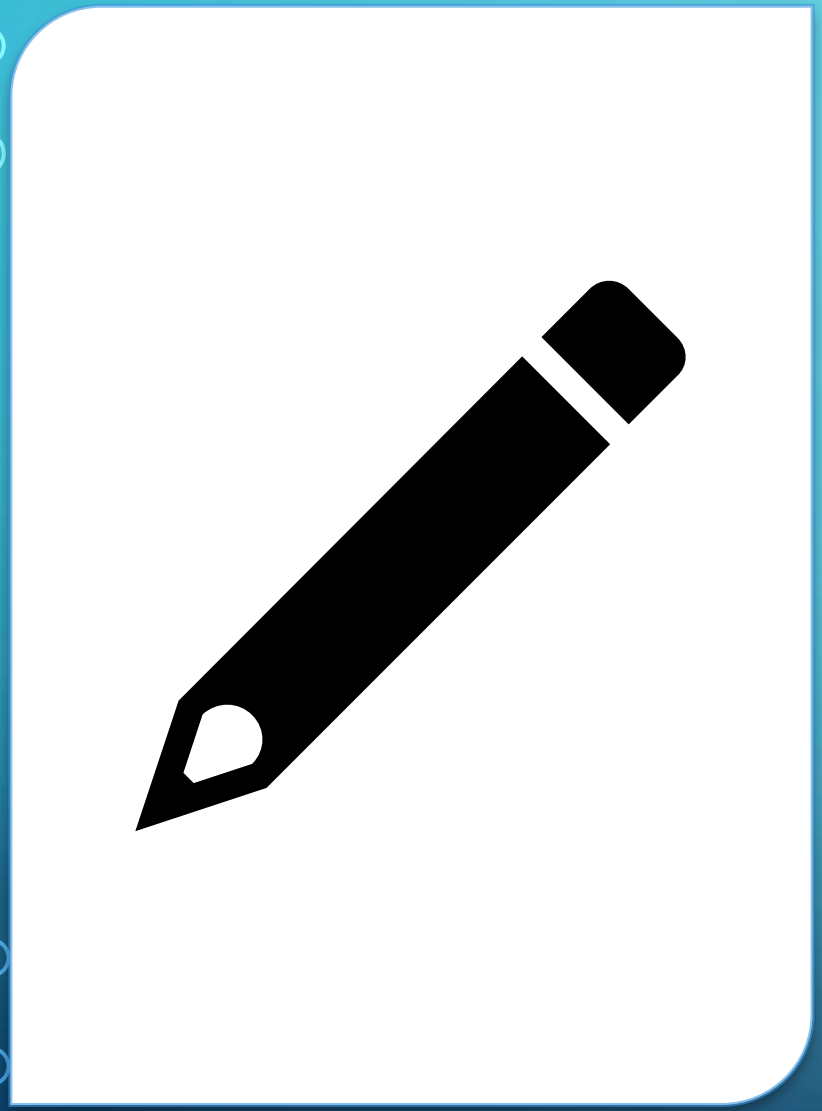
INTRUSIONES	
Clasificación	**Tipo**
Según su naturaleza	Intrusiones de uso erróneo
	Intrusiones de anomalía
Según el modo de acceso al sistema	Intrusión física
	Intrusión del sistema
	Intrusión alejada



Ejemplo.

REALIZANDO UN CONTROL RUTINARIO SE HA DADO CUENTA DE QUE HAY UNA APLICACIÓN QUE TIENE UN COMPORTAMIENTO ANÓMALO Y DETECTA QUE ES POSIBLE QUE HAYA HABIDO UNA INTRUSIÓN PROCEDENTE DEL EXTERIOR.

¿QUÉ TIPO DE INTRUSIÓN PUEDE HABERSE DETECTADO? INDÍQUELA ATENDIENDO A SU NATURALEZA Y AL MODO DE ACCESO AL SISTEMA.



Ejemplo. Solución

POR UN LADO LAS INTRUSIONES QUE PROVOCAN COMPORTAMIENTOS INUSUALES EN EL SISTEMA O EN ALGUNA DE SUS APLICACIONES SE CLASIFICAN COMO INTRUSIONES DE ANOMALÍA.

POR EL OTRO LADO, AQUELLAS INTRUSIONES QUE PROVIENEN DEL EXTERIOR Y QUE POR TANTO SE HAN PRODUCIDO DE MODO REMOTO ESTÁN TIPIFICADAS COMO INTRUSIONES ALEJADAS.

6.1. CLASIFICACIÓN DE LOS INTENTOS DE INTRUSIÓN SEGÚN SU IMPACTO

El impacto sobre los activos de la organización de una intrusión es uno de los elementos fundamentales a tener en cuenta para su clasificación.

6.1. CLASIFICACIÓN DE LOS INTENTOS DE INTRUSIÓN SEGÚN SU IMPACTO

Intentos de entrada

Los intentos de entrada se producen cuando hay usuarios no autorizados que pretenden acceder al sistema para llevar a cabo acciones malintencionadas.

El impacto de esta intrusión puede considerarse alto ya que, si este usuario consigue acceder y obtener los privilegios apropiados, puede llegar a dañar el sistema en su totalidad.

6.1. CLASIFICACIÓN DE LOS INTENTOS DE INTRUSIÓN SEGÚN SU IMPACTO

Ataques enmascarados

En este caso no se trata de usuarios nuevos que intentan acceder al sistema. Aquí el intruso utiliza usuarios ya registrados a través de los cuales intentar atacar.

El impacto de este tipo de intrusión es inferior a los intentos de entrada, ya que cabe la posibilidad de que el usuario a través del que se accede al sistema tenga menos privilegios y, por lo tanto, el daño que pueda realizar sea menor.

6.1. CLASIFICACIÓN DE LOS INTENTOS DE INTRUSIÓN SEGÚN SU IMPACTO

Penetraciones en el sistema de control

En las penetraciones en el sistema de control los intrusos intentan acceder a las herramientas de control del sistema con el fin de alterarlas.

Las penetraciones pueden ser:

- **Internas**: si se producen desde el mismo sistema.
- **Externas**: si proceden de otro equipo o de la red.

Su impacto puede ser alto, ya que los procesos de control de un sistema suelen controlar todos los demás procesos, usuarios, rendimientos y demás características y contenidos del equipo al que se está administrando.

6.1. CLASIFICACIÓN DE LOS INTENTOS DE INTRUSIÓN SEGÚN SU IMPACTO

Denegación de servicio

Los intrusos que acceden al sistema de una organización con ataques de denegación de servicio (DoS o Denial of Service) tienen como objetivo limitar e incluso impedir el acceso a los recursos y servicios de una organización durante un período de tiempo indeterminado o indefinido.

Su impacto es bajo, ya que aunque impide la actividad habitual de una organización no hay alteración ni borrado de datos. Lo habitual es que estos ataques se lleven a cabo para dañar la imagen y reputación de las organizaciones al impedir que los clientes puedan acceder a ellas y que estas no puedan ofrecer sus servicios con facilidad.

6.1. CLASIFICACIÓN DE LOS INTENTOS DE INTRUSIÓN SEGÚN SU IMPACTO

Uso malicioso

Los ataques por uso malicioso se producen cuando el intruso se infiltra o causa daños en un equipo o sistema sin autorización.

Dependiendo del tipo de software malicioso o malware utilizado el impacto será distinto: desde saturación de servidores, borrado de datos, aparición de ventanas molestas, observación de actividad, envío de spam, etc.

6.1. CLASIFICACIÓN DE LOS INTENTOS DE INTRUSIÓN SEGÚN SU IMPACTO

Resumen

Tipo de intrusión	Impacto
Intentos de entrada	Alto
Penetraciones en el sistema de control	Alto
Ataques enmascarados	Medio
Fuga	Bajo
Denegación de servicio	Bajo

7. ESTABLECIMIENTO DEL NIVEL DE INTERVENCIÓN REQUERIDO EN FUNCIÓN DEL IMPACTO PREVISIBLE

El impacto previsible de una intrusión viene determinado también por los efectos negativos producidos o potenciales que se pueden originar y por la criticidad de los recursos que se van a ver afectados por dicha intrusión.

7.1. CLASIFICACIÓN DE LOS INCIDENTES SEGÚN SU NIVEL DE CRITICIDAD

El Esquema Nacional de Seguridad clasifica:

Nivel	Nombre
5	CRÍTICO
4	MUY ALTO
3	ALTO
2	MEDIO
1	BAJO/NULO

7.1. CLASIFICACIÓN DE LOS INCIDENTES SEGÚN SU NIVEL DE CRITICIDAD

Nivel de criticidad crítico

En este nivel se encuentran las intrusiones de las que se tiene constancia que han producido un impacto muy significativo, afectando tanto a la confidencialidad, como a la disponibilidad o a la integridad de los datos.

7.1. CLASIFICACIÓN DE LOS INCIDENTES SEGÚN SU NIVEL DE CRITICIDAD

Nivel de criticidad muy alto

Tienen nivel de criticidad muy alto las intrusiones de las que se tiene constancia que han producido un impacto considerable (y no muy significativo) en recursos clasificados como críticos.

7.1. CLASIFICACIÓN DE LOS INCIDENTES SEGÚN SU NIVEL DE CRITICIDAD

Nivel de criticidad alto

Las intrusiones con nivel de criticidad alto son aquellas que tienen un impacto considerable en recursos e información considerados como no críticos por la organización.

7.1. CLASIFICACIÓN DE LOS INCIDENTES SEGÚN SU NIVEL DE CRITICIDAD

Nivel de criticidad medio

El impacto de las intrusiones con nivel de criticidad medio es limitado y afecta a recursos e información considerados como no críticos.

7.1. CLASIFICACIÓN DE LOS INCIDENTES SEGÚN SU NIVEL DE CRITICIDAD

Nivel de criticidad bajo

Las intrusiones de criticidad bajo tienen un impacto nulo o insignificante para las organizaciones y suelen ser detectadas y erradicadas por sus sistemas y herramientas de seguridad.

7.1. CLASIFICACIÓN DE LOS INCIDENTES SEGÚN SU NIVEL DE CRITICIDAD

Resumen

Nivel de criticidad	Impacto	Recursos afectados
CRÍTICO	MUY CONSIDERABLE	CRÍTICOS
MUY ALTO	CONSIDERABLE	CRÍTICOS
ALTO	CONSIDERABLE	NO CRÍTICOS
MEDIO	LIMITADO	NO CRÍTICOS
BAJO	NULO	NO CRÍTICOS

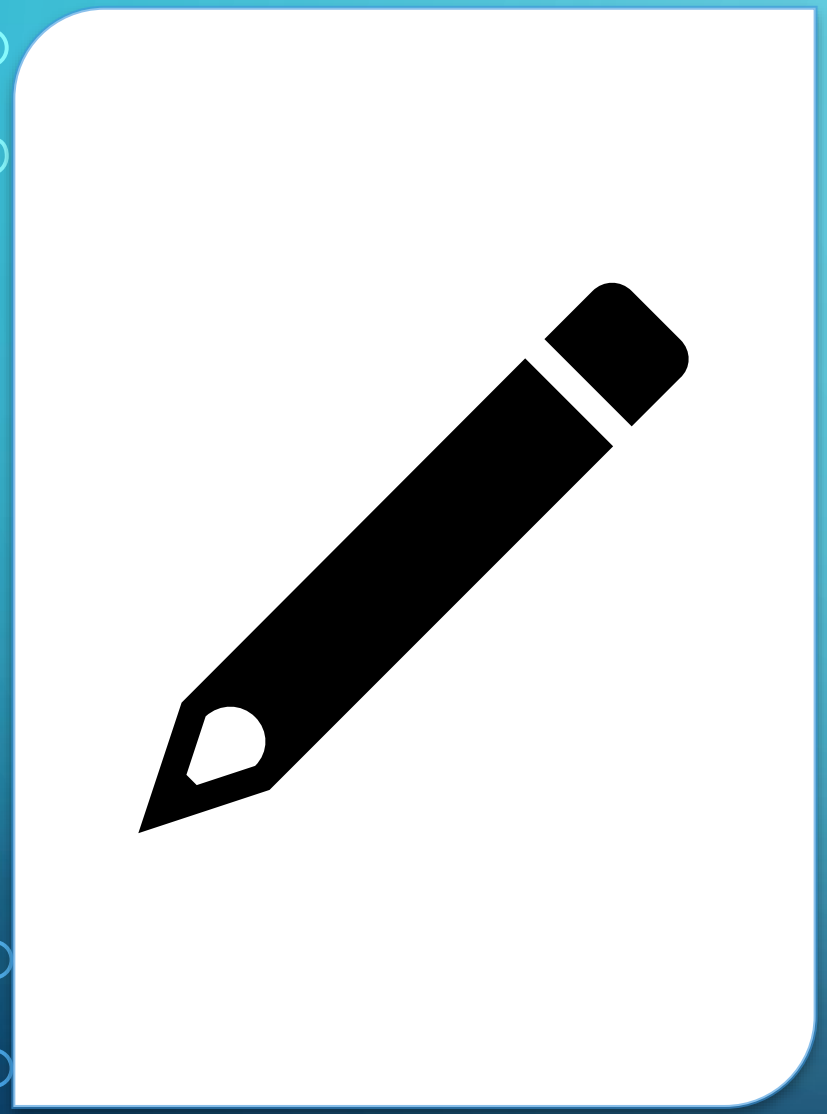
7.2. NIVEL DE INTERVENCIÓN REQUERIDO EN FUNCIÓN DEL IMPACTO Y CRITICIDAD DE LA INTRUSIÓN

Nivel de criticidad	Tiempo máximo para su registro
CRÍTICO	1 hora
MUY ALTO	12 horas
ALTO	24 horas
MEDIO	1 semana
BAJO	1 mes

7.2. NIVEL DE INTERVENCIÓN REQUERIDO EN FUNCIÓN DEL IMPACTO Y CRITICIDAD DE LA INTRUSIÓN

Intervención para la contención y erradicación de la intrusión según su impacto y criticidad

Nivel de criticidad	Plazo máximo de contención	Plazo máximo de erradicación
CRÍTICO	8 horas	24 horas
MUY ALTO	48 horas	72 horas
ALTO	4 días naturales	14 días naturales
MEDIO	1 mes	1 mes
BAJO	3 meses	3 meses



Ejemplo.

EL SISTEMA DE DETECCIÓN DE INTRUSIONES HA DETECTADO UNA INTRUSIÓN QUE PUEDE OCASIONAR UN IMPACTO CONSIDERABLE EN LOS RECURSOS CRÍTICOS DE LA ORGANIZACIÓN.

¿CUÁL ES EL NIVEL DE CRITICIDAD DEL INCIDENTE Y QUÉ TIEMPO DE REGISTRO MÁXIMO DEBERÍA PASAR? ¿POR QUÉ ES IMPORTANTE NO SOBREPASARLO?

Ejemplo. Solución

LAS INTRUSIONES CON IMPACTO CONSIDERABLE EN RECURSOS CRÍTICOS SE CORRESPONDEN CON UN NIVEL DE CRITICIDAD MUY ELEVADO.

EL TIEMPO MÁXIMO DE RESPUESTA PARA LAS INTRUSIONES CLASIFICADAS EN UN NIVEL DE CRITICIDAD MUY ALTO ESTÁ EN 12 HORAS Y, AUNQUE EN OCASIONES MUY ESPECIALES SE PODRÍA SOBREPASAR, NO ES RECOMENDABLE TARDAR MÁS PARA EVITAR LA PROPAGACIÓN DE LOS EFECTOS PERJUDICIALES DE LA INTRUSIÓN A LOS RECURSOS CRÍTICOS ELEVANDO SU GASTO DE RECUPERACIÓN Y PUDIENDO PROVOCAR DAÑOS IRREVERSIBLES.