# IFCT0109. SEGURIDAD INFORMÁTICA

# MF0488_3 GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

# UD05

## UNIDAD 05. PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN



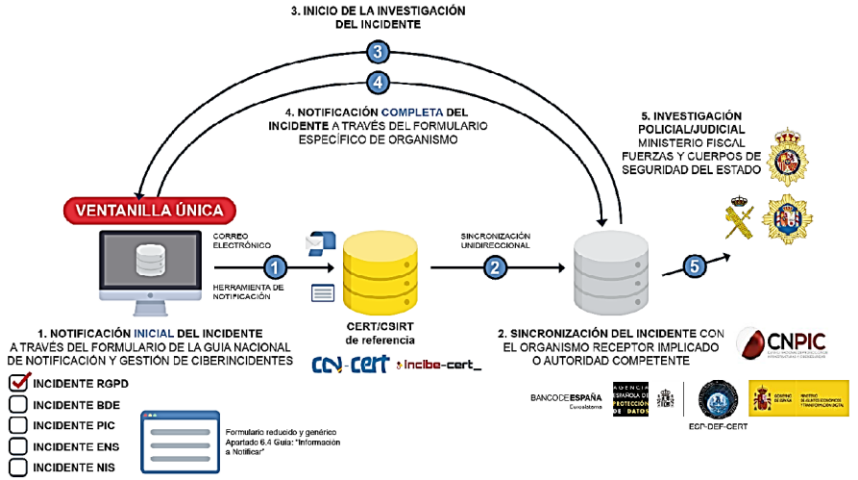
DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

# CONTENIDOS

1. **INTRODUCCIÓN**
2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES
3. CATEGORIZACIÓN DE LOS INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES EN FUNCIÓN DE SU IMPACTO POTENCIAL
4. CRITERIOS PARA LA DETERMINACIÓN DE LAS EVIDENCIAS OBJETIVAS EN LAS QUE SE SOPORTARÁ LA GESTIÓN DEL INCIDENTE
5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES
6. GUÍA PARA LA CLASIFICACIÓN Y ANÁLISIS INICIAL DEL INTENTO DE INTRUSIÓN O INFECCIÓN CONTEMPLANDO EL IMPACTO PREVISIBLE DEL MISMO
7. ESTABLECIMIENTO DEL NIVEL DE INTERVENCIÓN REQUERIDO EN FUNCIÓN DEL IMPACTO PREVISIBLE
8. GUÍA PARA LA INVESTIGACIÓN Y DIAGNÓSTICO DEL INCIDENTE DE INTENTO DE INTRUSIÓN O INFECCIONES
9. ESTABLECIMIENTO DEL PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE LOS SISTEMAS TRAS UN INCIDENTE DERIVADO DE UN INTENTO DE INTRUSIÓN O INFECCIÓN
10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE
11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE Y LOS REGISTROS NECESARIOS PARA DOCUMENTAR EL HISTÓRICO DEL INCIDENTE

# 1. INTRODUCCIÓN

CUANDO SE DETECTA UN **INTENTO DE INTRUSIÓN** ES RECOMENDABLE SEGUIR UN **PROCEDIMIENTO DEFINIDO CLARAMENTE** PARA QUE LA GESTIÓN DE DICHA INTRUSIÓN SE REALICE CORRECTAMENTE Y SE MINIMICEN TODO LO POSIBLE SUS EFECTOS NEGATIVOS.



# 1. INTRODUCCIÓN

EN ESTE PROCEDIMIENTO HAY QUE **DESIGNAR A UNA SERIE DE RESPONSABLES ENCARGADOS DE LA GESTIÓN DE LA INTRUSIÓN** O DE LA INCIDENCIA QUE REALICEN BÚSQUEDAS DE INFORMACIÓN ADICIONAL PARA **CONFIRMAR LA INTRUSIÓN O PARA DECLARARLA COMO UNA FALSA ALARMA**.

# 1. INTRODUCCIÓN

SI **LA INCIDENCIA** SE DECLARA REAL **DEBERÁ CATEGORIZARSE SEGÚN SU IMPACTO POTENCIAL Y RECOGERSE DETALLES** SOBRE CÓMO HA PODIDO ACCEDER EN EL SISTEMA Y HA EVOLUCIONADO DESDE QUE SE DETECTÓ.

SE COMENTAN TODAS LAS **FASES DE GESTIÓN DE INTENTOS DE INTRUSIÓN**: DESDE LA DETECCIÓN DE INDICIOS HASTA SU CIERRE, PASANDO POR EL CONTROL QUE HAY QUE LLEVAR A CABO A LO LARGO DE TODA LA GESTIÓN.

CON ESTO, **SERÁ POSIBLE DEFENDERSE** ANTE LA PRESENCIA DE **INTRUSIONES Y GESTIONAR LOS RECURSOS** DE LA EMPRESA **PARA CONTENER LOS DAÑOS Y CONSEGUIR ERRADICAR LAS INCIDENCIAS** EN EL MENOR TIEMPO POSIBLE.

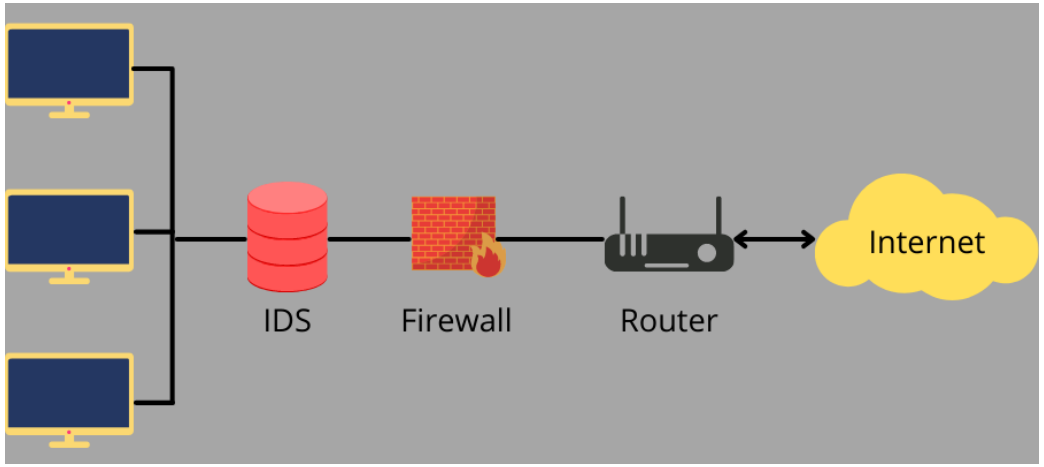
# CONTENIDOS

1. INTRODUCCIÓN
2. **ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES**
3. CATEGORIZACIÓN DE LOS INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES EN FUNCIÓN DE SU IMPACTO POTENCIAL
4. CRITERIOS PARA LA DETERMINACIÓN DE LAS EVIDENCIAS OBJETIVAS EN LAS QUE SE SOPORTARÁ LA GESTIÓN DEL INCIDENTE
5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES
6. GUÍA PARA LA CLASIFICACIÓN Y ANÁLISIS INICIAL DEL INTENTO DE INTRUSIÓN O INFECCIÓN CONTEMPLANDO EL IMPACTO PREVISIBLE DEL MISMO
7. ESTABLECIMIENTO DEL NIVEL DE INTERVENCIÓN REQUERIDO EN FUNCIÓN DEL IMPACTO PREVISIBLE
8. GUÍA PARA LA INVESTIGACIÓN Y DIAGNÓSTICO DEL INCIDENTE DE INTENTO DE INTRUSIÓN O INFECCIONES
9. ESTABLECIMIENTO DEL PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE LOS SISTEMAS TRAS UN INCIDENTE DERIVADO DE UN INTENTO DE INTRUSIÓN O INFECCIÓN
10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE
11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE Y LOS REGISTROS NECESARIOS PARA DOCUMENTAR EL HISTÓRICO DEL INCIDENTE

# 2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES

PARA EVITAR Y PREVENIR LAS INTRUSIONES SE UTILIZAN HERRAMIENTAS COMO *CORTAFUEGOS Y SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSIONES O IDS/IPS.*

**LA ELECCIÓN DEL IDS/IPS CORRECTO ES UNA DECISIÓN DE GRAN RESPONSABILIDAD** POR LAS CONSECUENCIAS DE LAS QUE PUEDE DERIVAR UNA MALA ELECCIÓN.



# 2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES

POR ELLO SE RECOMIENDA SEGUIR UNA SERIE DE CRITERIOS EN EL MOMENTO DE REALIZAR LA ELECCIÓN:

- **ESCALABILIDAD**
- **FIRMAS DE ATAQUE UTILIZADAS**
- **CAPACIDAD DE ADMINISTRACIÓN Y GESTIÓN**
- **TIPO DE ESTRUCTURA DE HARDWARE UTILIZADA**

# 2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES

## ESCALABILIDAD

***CAPACIDAD DE LA HERRAMIENTA DE ADAPTARSE A LOS CAMBIOS DE TRÁFICO DE LA RED***. ES RECOMENDABLE QUE LOS IDS/IPS SIGAN FUNCIONANDO CORRECTAMENTE TANTO A NIVELES MÍNIMOS DE TRÁFICO DE RED COMO EN MOMENTOS DE HORA PUNTA EN EL QUE EL TRÁFICO ES MUCHO MÁS ELEVADO.

## FIRMAS DE ATAQUE UTILIZADAS

LOS IDS/IPS ***SON DE MAYOR CALIDAD CUANDO UTILIZAN UN MAYOR NÚMERO DE FIRMAS DE ATAQUE*** PORQUE SE REDUCEN LAS POSIBILIDADES DE OBTENER FALSOS POSITIVOS O NEGATIVOS AL DISPONER DE UNA BASE DE DATOS DE ATAQUES MÁS AMPLIA.

# 2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES

## CAPACIDAD DE ADMINISTRACIÓN Y GESTIÓN

***CUANTAS MÁS FUNCIONALIDADES DE AUTOGESTIÓN Y DE ADMINISTRACIÓN TENGA, MÁS SENCILLA SERÁ SU UTILIZACIÓN***. SE RECOMIENDA HERRAMIENTAS QUE TENGAN FUNCIONES PROPIAS DE EXAMEN DE LOGS, CAPACIDAD DE ARCHIVO, GESTIÓN DE ALARMAS, CONSOLA CENTRALIZADA, ETC.

## TIPO DE ESTRUCTURA DE HARDWARE UTILIZADA

***LA TOPOLOGÍA DE LA RED Y LA DISPOSICIÓN DE LOS EQUIPOS Y CORTAFUEGOS*** TAMBIÉN SON UNOS ***ELEMENTOS A TENER EN CUENTA*** EN EL MOMENTO DE ***ELEGIR EL IDS/IPS*** ADECUADO. ATENDIENDO A LA UBICACIÓN DEL CORTAFUEGOS PUEDE INTERESAR UN IDS/IPS CON FUNCIONALIDADES DISTINTAS.

# 2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES

## RESPONSABILIDADES DE GESTIÓN Y NOTIFICACIÓN DE INTRUSIONES

LAS ORGANIZACIONES DEBEN ESTABLECER UN **PROCEDIMIENTO DE GESTIÓN Y NOTIFICACIÓN DE INTRUSIONES PARA QUE EL TIEMPO DE RESPUESTA SEA LO MÁS REDUCIDO POSIBLE Y LOS DAÑOS PRODUCIDOS SEAN LOS MÍNIMOS**.

ES NECESARIA LA **DESIGNACIÓN DE RESPONSABLES** CUYA FUNCIÓN PRINCIPAL SEA LA DE **LOCALIZAR LAS INTRUSIONES** DETECTADAS POR LOS SISTEMAS DE PROTECCIÓN Y **REMITIR LA INFORMACIÓN** A LAS PERSONAS ADECUADAS Y ENCARGADAS DE TOMAR MEDIDAS DE RESPUESTA ANTE EL INCIDENTE O INTRUSIÓN.

# 2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES

## RESPONSABILIDADES DE GESTIÓN Y NOTIFICACIÓN DE INTRUSIONES

DE ESTE MODO, **LAS ORGANIZACIONES DEBERÁN FORMAR UNA ESTRUCTURA INTEGRADA POR VARIAS ÁREAS** QUE SEA **CAPAZ DE**:

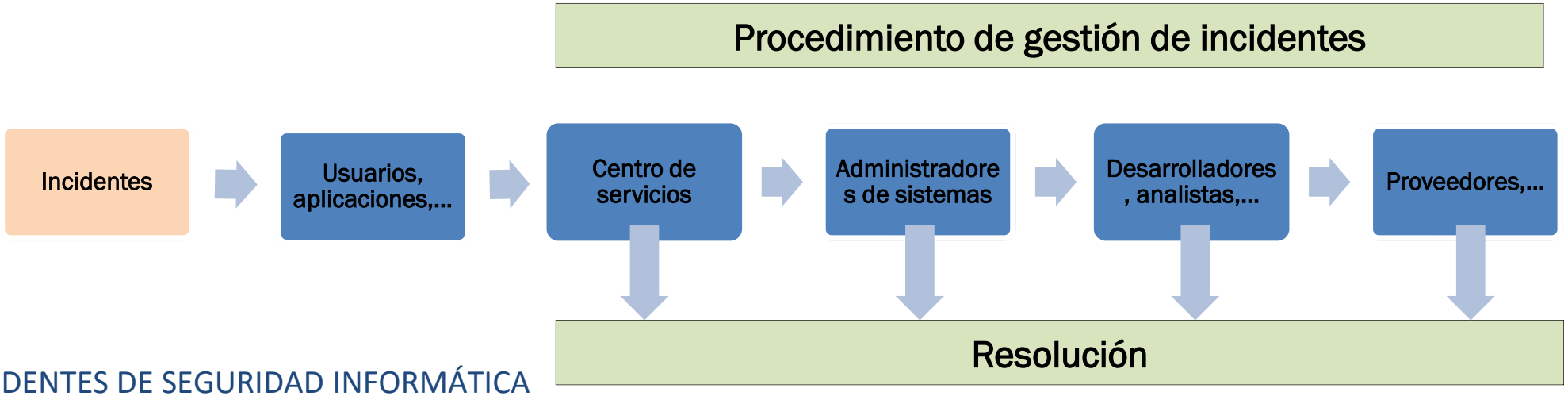
- **DETECTAR** CUALQUIER ALTERACIÓN DE LOS SERVICIOS OFRECIDOS POR LA ORGANIZACIÓN.
- **REGISTRAR Y CLASIFICAR** ESTOS INCIDENTES.
- **ASIGNAR AL PERSONAL** ENCARGADO DE RESTAURAR LA SITUACIÓN AL PUNTO PREVIO DE LA PRODUCCIÓN DEL INCIDENTE.

# 2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES

## RESPONSABILIDADES DE GESTIÓN Y NOTIFICACIÓN DE INTRUSIONES

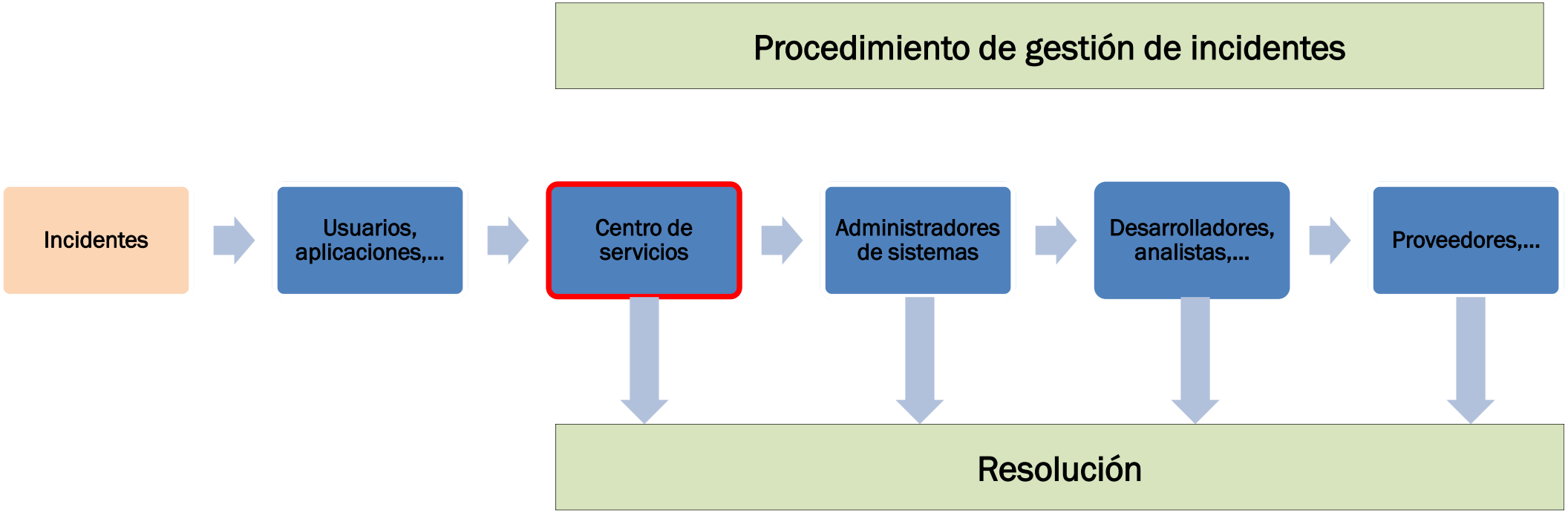
EL PROCESO **DE GESTIÓN DE INCIDENTES DEBE ATENDER A UNA ESTRUCTURA** SIMILAR A LA QUE SE MUESTRA EN LA IMAGEN:

COMO SE MUESTRA EN LA IMAGEN, EN EL MOMENTO QUE LOS USUARIOS O APLICACIONES DETECTAN UNA INTRUSIÓN **HAY VARIAS ÁREAS QUE SE PUEDEN ENCARGAR DE LLEVAR A CABO SU GESTIÓN**:



# 2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES

## RESPONSABILIDADES DE GESTIÓN Y NOTIFICACIÓN DE INTRUSIONES



# 2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES

## RESPONSABILIDADES DE GESTIÓN Y NOTIFICACIÓN DE INTRUSIONES

### CENTRO DE SERVICIOS

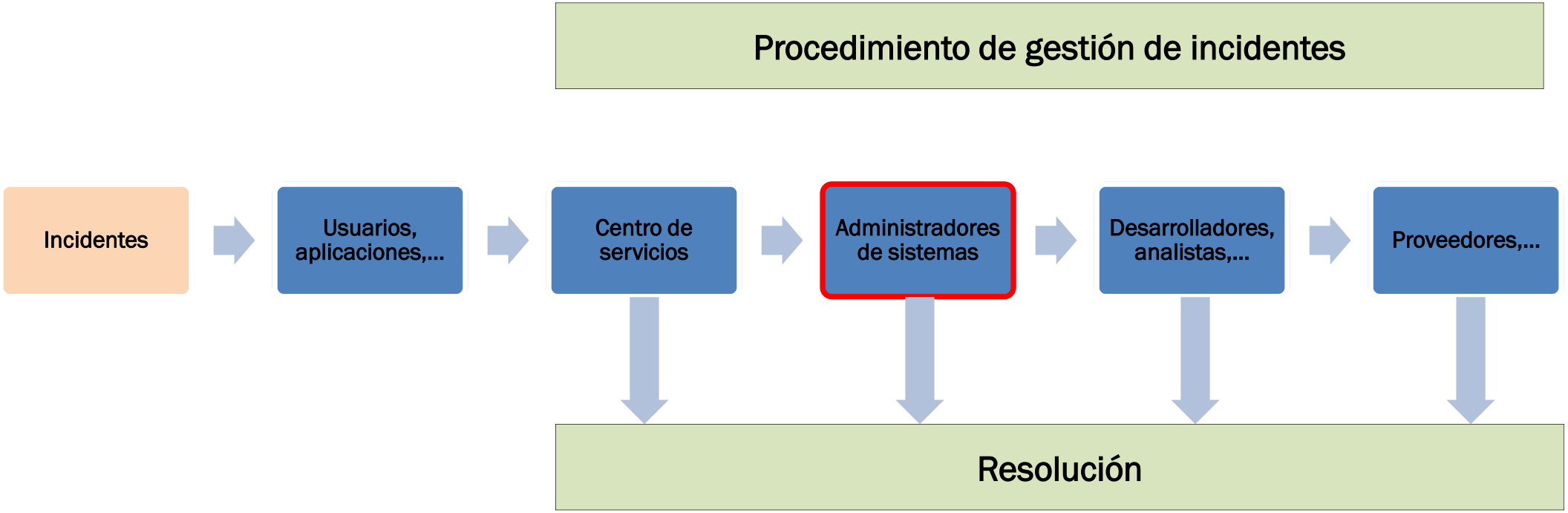
ES EL **PRIMER NIVEL** DE GESTIÓN DE INTRUSIONES, EL **PUNTO DE CONTACTO ENTRE LOS USUARIOS Y LA GESTIÓN** DE ÉSTAS. DA SOPORTE EN LA GESTIÓN REALIZANDO FUNCIONES COMO:

- REGISTRO Y MONITORIZACIÓN DE INCIDENTES.
- APLICACIÓN DE SOLUCIONES TEMPORALES Y PROVISIONALES ANTE ATAQUES E INTRUSIONES.
- COLABORAN CON NIVELES SUPERIORES EN LA ELABORACIÓN DE BASES DE DATOS DE INTRUSIONES.

SON EL PRIMER PUNTO DE CONTACTO CON LA INTRUSIÓN Y **SE ENCARGAN DE RESOLVER PROBLEMAS BÁSICOS E INTRUSIONES SENCILLAS DE COMBATIR**.

# 2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES

## RESPONSABILIDADES DE GESTIÓN Y NOTIFICACIÓN DE INTRUSIONES



# 2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES

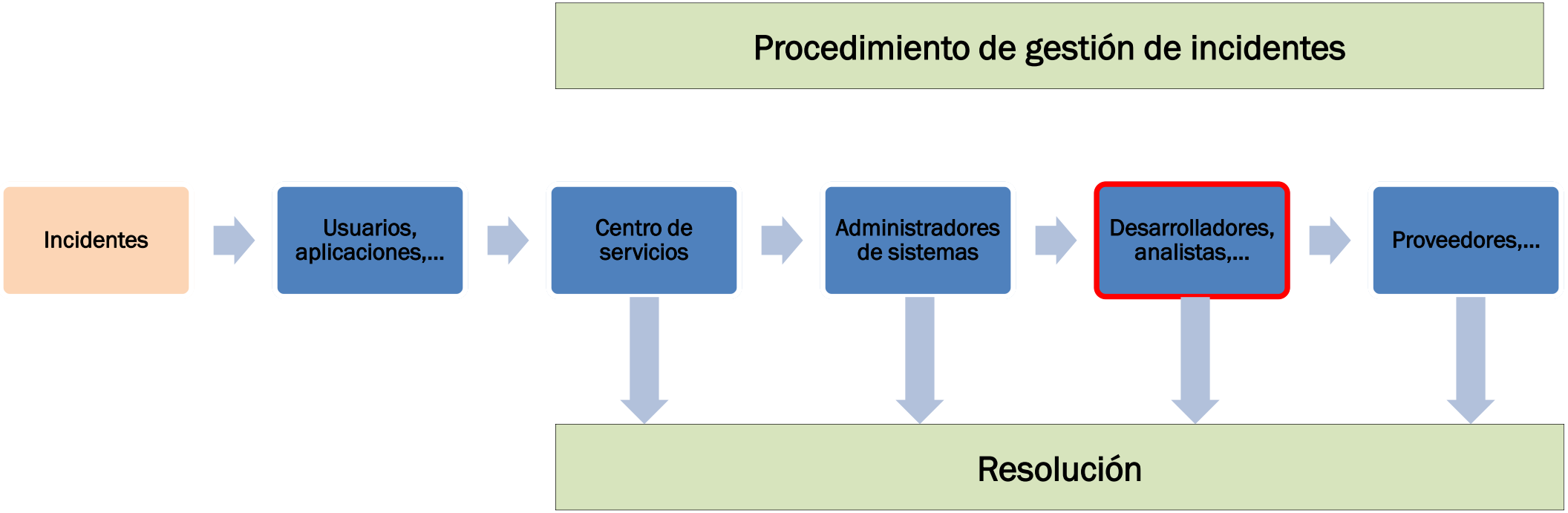
## RESPONSABILIDADES DE GESTIÓN Y NOTIFICACIÓN DE INTRUSIONES

### ADMINISTRADORES DE SISTEMAS

TIENEN **UN CONOCIMIENTO MÁS PROFUNDO DEL FUNCIONAMIENTO DE LAS INTRUSIONES Y ATAQUES** Y LOS QUE REALMENTE SON CAPACES DE DESARROLLAR RESPUESTAS RÁPIDAS ANTE ATAQUES MÁS COMPLEJOS.

# 2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES

## RESPONSABILIDADES DE GESTIÓN Y NOTIFICACIÓN DE INTRUSIONES



# 2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES

## RESPONSABILIDADES DE GESTIÓN Y NOTIFICACIÓN DE INTRUSIONES

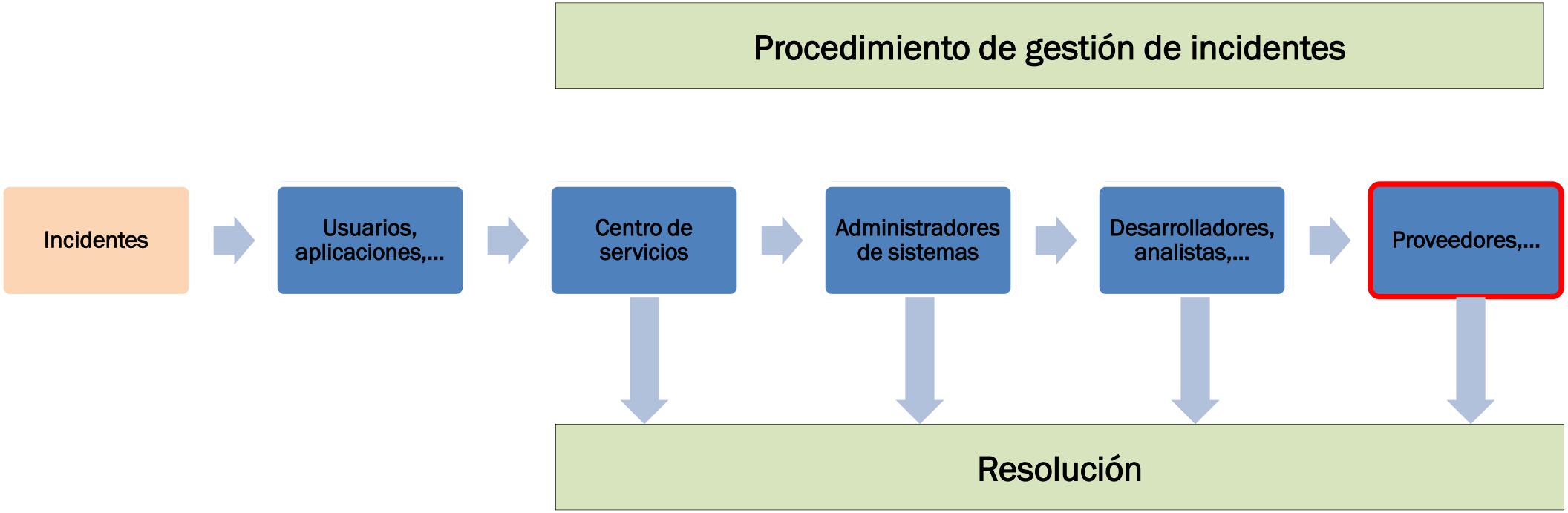
### DESARROLLADORES Y ANALISTAS

TIENEN **CONOCIMIENTOS AVANZADOS SOBRE LAS POSIBLES INTRUSIONES QUE PUEDEN ACCEDER AL SISTEMA, SU COMPORTAMIENTO Y SU FUNCIONAMIENTO INTERNO**.

PUEDEN **DESARROLLAR HERRAMIENTAS** DE CONTRAATAQUE Y PROTECCIÓN AVANZADA ANTE INTRUSIONES DESCONOCIDAS.

# 2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES

## RESPONSABILIDADES DE GESTIÓN Y NOTIFICACIÓN DE INTRUSIONES



# 2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES

## RESPONSABILIDADES DE GESTIÓN Y NOTIFICACIÓN DE INTRUSIONES

### PROVEEDORES

SON EL **ÚLTIMO ESCALÓN**, **CUANDO LA ORGANIZACIÓN NO HA SIDO CAPAZ DE COMBATIR EL INCIDENTE** SOLO QUEDA ACUDIR AL PROVEEDOR DE LA HERRAMIENTA DEL IDS/IPS IMPLANTADA PARA QUE, CON CONSULTAS AVANZADAS EN SUS BASES DE DATOS, PUEDAN FACILITAR UNA SOLUCIÓN AL PROBLEMA.

# 2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES

## RESPONSABILIDADES DE GESTIÓN Y NOTIFICACIÓN DE INTRUSIONES

**EL NIVEL DE COMPLEJIDAD DE LA INTRUSIÓN DETERMINARÁ LA DERIVACIÓN DE LA MISMA A UN NIVEL U OTRO DE LA ORGANIZACIÓN** PARA ENCARGARSE DE SU ERRADICACIÓN Y DE RESTAURAR LOS SISTEMAS.

A **MAYOR COMPLEJIDAD** DE LA INTRUSIÓN, **MAYORES SERÁN LOS CONOCIMIENTOS** QUE DEBERÁN TENER LOS RESPONSABLES DE SU ERRADICACIÓN Y, POR LO TANTO, MÁS ALTO SERÁ EL NIVEL AL QUE SE DEBERÁ NOTIFICAR SU APARICIÓN.

UNA **CORRECTA DESIGNACIÓN DE RESPONSABILIDADES Y UNA ELECCIÓN ADECUADA DE LA NOTIFICACIÓN** DE POSIBLES INTRUSIONES PUEDE INFLUIR SIGNIFICATIVAMENTE EN EL TIEMPO DE RESPUESTA A LA INTRUSIÓN.

# 2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES

## OBLIGACIONES LEGALES DE GESTIÓN Y NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD E INTRUSIONES

EN ESPAÑA HAY UNA ESPECIAL **PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL** CON EL **RGPD** Y LA **LOPDGDD.**

ESTA NORMATIVA HABLA DE LA **GESTIÓN DE INCIDENTES QUE AFECTEN A DATOS DE CARÁCTER PERSONAL Y DE LA DESIGNACIÓN DE RESPONSABLES** DE FICHEROS QUE CONTENGAN DATOS DE CARÁCTER PERSONAL DE SU DETECCIÓN, NOTIFICACIÓN Y GESTIÓN.

TODO DEBE QUEDAR PLASMADO EN EL **DOCUMENTO DE SEGURIDAD**. ATENDIENDO AL NIVEL DE SEGURIDAD DE LA INFORMACIÓN, EL PROCEDIMIENTO SERÁ DISTINTO.

# 2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES

## OBLIGACIONES LEGALES DE GESTIÓN Y NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD E INTRUSIONES

EN LAS **MEDIDAS DE SEGURIDAD BÁSICAS** *EL PROCEDIMIENTO DE NOTIFICACIÓN Y GESTIÓN DE INCIDENCIAS* ***DEBERÁ CONTENER NECESARIAMENTE UN REGISTRO*** EN EL QUE SE HAGA CONSTAR:

- EL TIPO DE INCIDENCIA.
- EL MOMENTO EN EL QUE SE HA PRODUCIDO LA INCIDENCIA.
- LA PERSONA QUE REALIZA LA NOTIFICACIÓN.
- A QUIÉN SE LE COMUNICA.
- LOS EFECTOS QUE HAN DERIVADO DE LA MISMA.

# 2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES

## OBLIGACIONES LEGALES DE GESTIÓN Y NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD E INTRUSIONES

EN LAS **MEDIDAS DE SEGURIDAD DE NIVEL MEDIO** EL PROCEDIMIENTO ***DEBERÁ INDICAR****, ADEMÁS DE LO DEL NIVEL BÁSICO****, LOS PROCEDIMIENTOS DE RECUPERACIÓN DE LOS DATOS REALIZADOS*** CONSTATANDO:

- LA PERSONA QUE EJECUTÓ EL PROCESO.
- LOS DATOS RESTAURADOS.
- EN SU CASO, QUÉ DATOS HAN SIDO NECESARIOS GRABAR MANUALMENTE EN EL PROCESO DE RECUPERACIÓN.

EL **RGPD** EXIGE ADEMÁS LA AUTORIZACIÓN DEL RESPONSABLE DEL FICHERO PARA LA EJECUCIÓN DE LOS PROCEDIMIENTOS DE RECUPERACIÓN DE LOS DATOS.

# 2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES

## OBLIGACIONES LEGALES DE GESTIÓN Y NOTIFICACIÓN DE INCIDENTES DE SEGURIDAD E INTRUSIONES

EN CUANTO A LAS **MEDIDAS DE SEGURIDAD DE NIVEL ALTO** NO SE HABLA ESPECÍFICAMENTE DE PROCEDIMIENTOS DE NOTIFICACIÓN Y GESTIÓN DE INCIDENCIAS.

SOLO *CABE DESTACAR* ***LA EXIGENCIA DE CONSERVAR UNA COPIA DE RESPALDO Y QUE LOS PROCEDIMIENTOS DE RECUPERACIÓN DE LOS DATOS*** *ESTÉN EN UN LUGAR DIFERENTE DE AQUEL EN EL QUE SE ENCUENTREN LOS EQUIPOS INFORMÁTICOS*, AÑADIENDO UNA MAYOR PROTECCIÓN Y MÁS POSIBILIDADES DE ÉXITO PARA RESTAURAR LOS EQUIPOS A SITUACIONES ANTERIORES DE PRODUCIRSE CUALQUIER INTRUSIÓN.

# CONTENIDOS

1. INTRODUCCIÓN
2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES
3. **CATEGORIZACIÓN DE LOS INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES EN FUNCIÓN DE SU IMPACTO POTENCIAL**
4. CRITERIOS PARA LA DETERMINACIÓN DE LAS EVIDENCIAS OBJETIVAS EN LAS QUE SE SOPORTARÁ LA GESTIÓN DEL INCIDENTE
5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES
6. GUÍA PARA LA CLASIFICACIÓN Y ANÁLISIS INICIAL DEL INTENTO DE INTRUSIÓN O INFECCIÓN CONTEMPLANDO EL IMPACTO PREVISIBLE DEL MISMO
7. ESTABLECIMIENTO DEL NIVEL DE INTERVENCIÓN REQUERIDO EN FUNCIÓN DEL IMPACTO PREVISIBLE
8. GUÍA PARA LA INVESTIGACIÓN Y DIAGNÓSTICO DEL INCIDENTE DE INTENTO DE INTRUSIÓN O INFECCIONES
9. ESTABLECIMIENTO DEL PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE LOS SISTEMAS TRAS UN INCIDENTE DERIVADO DE UN INTENTO DE INTRUSIÓN O INFECCIÓN
10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE
11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE Y LOS REGISTROS NECESARIOS PARA DOCUMENTAR EL HISTÓRICO DEL INCIDENTE

# 3. CATEGORIZACIÓN DE LOS INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES EN FUNCIÓN DE SU IMPACTO POTENCIAL

LA **CLASIFICACIÓN DE UN INCIDENTE** TIENE COMO MISIÓN LA ***RECOPILACIÓN DE TODA LA INFORMACIÓN QUE PUEDA UTILIZARSE PARA SU RESOLUCIÓN Y PARA LA RESTAURACIÓN DEL SISTEMA.*** ESTE PROCESO DE CLASIFICACIÓN ES NECESARIO QUE CONTENGA, POR LO MENOS:

- **CATEGORIZACIÓN DEL INCIDENTE**
- **NIVEL DE PRIORIDAD**
- **ASIGNACIÓN DE RECURSOS**
- **MONITORIZACIÓN DEL ESTADO DEL INCIDENTE Y DEL TIEMPO DE RESPUESTA ESPERADO**

# 3. CATEGORIZACIÓN DE LOS INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES EN FUNCIÓN DE SU IMPACTO POTENCIAL

## CATEGORIZACIÓN DEL INCIDENTE

ASIGNARLE UNA CATEGORÍA SEGÚN EL **TIPO DE INCIDENTE** Y LOS RESPONSABLES DESIGNADOS PARA SU GESTIÓN.

## NIVEL DE PRIORIDAD

SEGÚN LOS **DAÑOS CAUSADOS Y LA URGENCIA** DEL INCIDENTE SE LE ASIGNARÁ UN NIVEL.

# 3. CATEGORIZACIÓN DE LOS INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES EN FUNCIÓN DE SU IMPACTO POTENCIAL

**ASIGNACIÓN DE RECURSOS:**

EN EL CASO DE QUE EL CENTRO DE SERVICIOS NO PUEDA COMBATIR LA INCIDENCIA DEBERÁN **DESIGNARSE TÉCNICOS ESPECIALIZADOS** Y RECURSOS ESPECÍFICOS PARA SU RESOLUCIÓN.

**MONITORIZACIÓN DEL ESTADO DEL INCIDENTE Y DEL TIEMPO DE RESPUESTA ESPERADO**

HAY QUE **ASOCIAR AL INCIDENTE UN ESTADO** (*DETECTADO, ACTIVO, RESUELTO, ETC.*) Y UN TIEMPO DE RESPUESTA Y RESOLUCIÓN ATENDIENDO A SUS NIVELES DE PRIORIDAD Y CRITICIDAD.

# 3. CATEGORIZACIÓN DE LOS INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES EN FUNCIÓN DE SU IMPACTO POTENCIAL

## TIPOS DE ATAQUES

ANTES DE CLASIFICAR EL INCIDENTE **HAY QUE SABER QUÉ TIPO DE ATAQUE SE ESTÁ PRODUCIENDO**.

EN UNA SITUACIÓN NORMAL EL FLUJO DE INFORMACIÓN CIRCULA DE ORIGEN A DESTINO SIN PROBLEMAS DE DISPONIBILIDAD, INTEGRIDAD Y ACCESIBILIDAD.

***CUANDO SE PRODUCE UN ATAQUE SE PIERDE ALGUNA DE LAS PROPIEDADES FUNDAMENTALES DE LA INFORMACIÓN***, MODIFICÁNDOSE DE ALGÚN MODO LA RECEPCIÓN DE LA INFORMACIÓN EN DESTINO.

# 3. CATEGORIZACIÓN DE LOS INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES EN FUNCIÓN DE SU IMPACTO POTENCIAL

## TIPOS DE ATAQUES

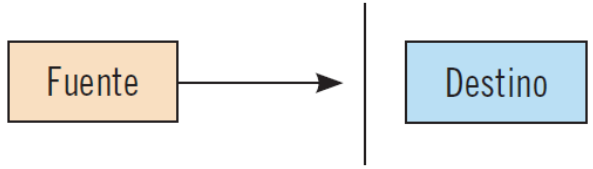
ATENDIENDO A ESTAS **MODIFICACIONES, LOS ATAQUES** DEBEN DISTINGUIRSE EN:

- **ATAQUES DE INTERRUPCIÓN**
- **ATAQUES DE INTERCEPCIÓN**
- **ATAQUES DE MODIFICACIÓN**
- **ATAQUES DE FABRICACIÓN**

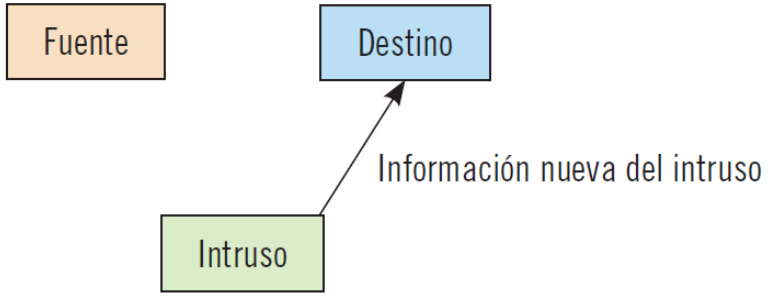
# 3. CATEGORIZACIÓN DE LOS INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES EN FUNCIÓN DE SU IMPACTO POTENCIAL

## TIPOS DE ATAQUES

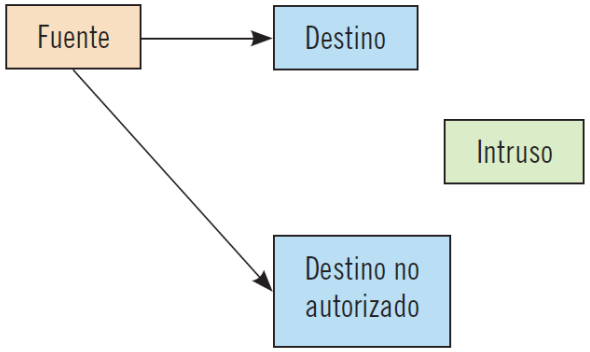
### ATAQUES DE INTERRUPCIÓN



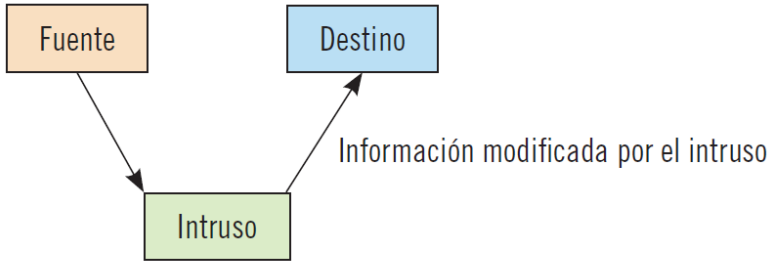

### ATAQUES DE FABRICACIÓN




### ATAQUES DE INTERCEPCIÓN




### ATAQUES DE MODIFICACIÓN



# 3. CATEGORIZACIÓN DE LOS INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES EN FUNCIÓN DE SU IMPACTO POTENCIAL

## TIPOS DE ATAQUES

### ATAQUES DE INTERRUPCIÓN

DESTRUYEN O INUTILIZAN LA INFORMACIÓN E INFLUYEN EN SU ACCESIBILIDAD Y/O DISPONIBILIDAD. EJEMPLOS: LA DESTRUCCIÓN DE ALGÚN DISPOSITIVO O LA SATURACIÓN DE LA CAPACIDAD DEL PROCESADOR CON EL FIN DE DIFICULTAR LA ACCESIBILIDAD DE LOS DATOS.

### ATAQUES DE INTERCEPCIÓN

USUARIOS NO AUTORIZADOS ACCEDEN A LOS DATOS DEL SISTEMA AFECTANDO A LA CONFIDENCIALIDAD DE LA INFORMACIÓN. POR EJEMPLO, REALIZACIÓN DE COPIAS DE INFORMACIÓN NO AUTORIZADAS O LA OBTENCIÓN DE CONTRASEÑAS.

# 3. CATEGORIZACIÓN DE LOS INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES EN FUNCIÓN DE SU IMPACTO POTENCIAL

## TIPOS DE ATAQUES

### ATAQUES DE MODIFICACIÓN:

USUARIOS NO AUTORIZADOS MODIFICAN LA INFORMACIÓN EN EQUIPOS ATACANDO A SU INTEGRIDAD. SON EJEMPLOS DE ATAQUES DE MODIFICACIÓN: CAMBIO DE CONTENIDOS DE BASES DE DATOS, CAMBIOS EN APLICACIONES, CAMBIOS EN DATOS BANCARIOS, ETC.

### ATAQUES DE FABRICACIÓN

LOS INTRUSOS EN ESTE CASO FALSIFICAN LA INFORMACIÓN DEL SISTEMA ATACANDO A SU AUTENTICIDAD. POR EJEMPLO, LA ADICIÓN DE CAMPOS O REGISTROS EN BASES DE DATOS Y LA ADICIÓN DE LÍNEAS DE UNA APLICACIÓN (ADICIÓN DE VIRUS, ETC.).

# 3. CATEGORIZACIÓN DE LOS INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES EN FUNCIÓN DE SU IMPACTO POTENCIAL

## TIPOS DE ATAQUES

A SU VEZ, SE PUEDEN CLASIFICAR EN **DOS GRUPOS**:

### ATAQUES PASIVOS

NO HAY ALTERACIÓN DE LA COMUNICACIÓN**. EL ATACANTE SE LIMITA A ESCUCHAR O MONITORIZAR EL TRÁFICO DE RED** PARA OBTENER LOS DATOS QUE SE ESTÁN TRANSMITIENDO. **SON DIFÍCILES DE DETECTAR.**

### ATAQUES ACTIVOS

EL ATACANTE **REALIZA ALGÚN TIPO DE ALTERACIÓN** DEL TRÁFICO DE RED, MODIFICÁNDOLO E INCLUSO CREANDO UN FALSO TRÁFICO. **SE PUEDEN DIVIDIR EN CUATRO CATEGORÍAS**:

# 3. CATEGORIZACIÓN DE LOS INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES EN FUNCIÓN DE SU IMPACTO POTENCIAL

## TIPOS DE ATAQUES

### ATAQUES ACTIVOS:

- **REACTUACIÓN:** SE CAPTURAN UNO O MÚLTIPLES MENSAJES LEGÍTIMOS PARA REPETIRLOS Y PRODUCIR EFECTOS NO DESEADOS POR EL USUARIO. UN EJEMPLO SERÍA LA REPETICIÓN DE TRANSFERENCIAS A UNA MISMA CUENTA SIN CONSENTIMIENTO DEL USUARIO.
- **MODIFICACIÓN DE MENSAJES:** SE ALTERA UNA PARTE DEL MENSAJE LEGÍTIMO PARA CONFUNDIR AL RECEPTOR DE LA INFORMACIÓN. POR EJEMPLO, SE PUEDE MODIFICAR UN MENSAJE TIPO “PARA COMPRAR EL LIBRO DEBE INGRESAR EL DINERO EN LA CUENTA X”, A OTRO MENSAJE “PARA COMPRAR EL LIBRO DEBE INGRESAR EL DINERO EN LA CUENTA Y” HACIENDO QUE EL RECEPTOR FINAL DEL DINERO NO SEA EL DESTINATARIO LEGÍTIMO.

# 3. CATEGORIZACIÓN DE LOS INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES EN FUNCIÓN DE SU IMPACTO POTENCIAL

## TIPOS DE ATAQUES

### ATAQUES ACTIVOS:

- **SUPLANTACIÓN DE IDENTIDAD O PHISHING:** EN ESTE CASO EL INTRUSO SIMULA SER OTRA ENTIDAD DIFERENTE. ES MUY HABITUAL LA DUPLICACIÓN DE PÁGINAS WEB BANCARIAS HACIÉNDOSE PASAR POR LA ENTIDAD REAL, CUANDO EN REALIDAD SE ESTÁN FACILITANDO DATOS CONFIDENCIALES A USUARIOS NO LEGÍTIMOS.
- **DEGRADACIÓN FRAUDULENTA DEL SERVICIO:** EL ATACANTE IMPIDE LA UTILIZACIÓN NORMAL DE LAS COMUNICACIONES Y DE LOS RECURSOS INFORMÁTICOS. POR EJEMPLO, SE PUEDE INTERRUMPIR EL SERVICIO DE UNA RED LANZÁNDOLE MULTITUD DE MENSAJES PARA SATURARLA.

# 3. CATEGORIZACIÓN DE LOS INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES EN FUNCIÓN DE SU IMPACTO POTENCIAL

## TIPOS DE ATAQUES

*LOS ATAQUES* ***DE INTERCEPCIÓN*** *SE CONSIDERAN* ***ATAQUES PASIVOS*** AL NO ALTERAR EL TRÁFICO DE RED

*LOS* ***ATAQUES DE INTERRUPCIÓN, MODIFICACIÓN Y FABRICACIÓN*** *SON* ***ATAQUES ACTIVOS*** AL ALTERAR LA INFORMACIÓN QUE SE PRETENDE TRANSMITIR.

# 3. CATEGORIZACIÓN DE LOS INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES EN FUNCIÓN DE SU IMPACTO POTENCIAL

## CATEGORIZACIÓN DE LOS INCIDENTES

UN FACTOR CLAVE ES LA **ELABORACIÓN DE PLANES DE CONTINGENCIA** QUE ANALICEN LOS EFECTOS DE POSIBLES INTRUSIONES Y LA DEFINICIÓN DE PROCEDIMIENTOS QUE PERMITAN MANTENER LA CIA DE LA INFORMACIÓN Y RECUPERAR EL MÁXIMO DE DATOS PERDIDOS POSIBLE.

EN ESTOS PLANES DE CONTINGENCIA ***DEBEN CONSIDERARSE LOS MEDIOS QUE SE VAN A UTILIZAR PARA CONTENER, ERRADICAR Y RECUPERAR EL SISTEMA ANTE INCIDENTES*** PARA QUE LA GESTIÓN DEL RIESGO SEA EFICAZ.

LO QUE NO PUEDE FALTAR EN UN PLAN DE CONTINGENCIA ES LA **CATEGORIZACIÓN DE LOS INCIDENTES** DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES SEGÚN SU IMPACTO POTENCIAL.

# 3. CATEGORIZACIÓN DE LOS INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES EN FUNCIÓN DE SU IMPACTO POTENCIAL

## CATEGORIZACIÓN DE LOS INCIDENTES

LA CATEGORIZACIÓN CONSISTIRÁ EN **CALCULAR LA PRIORIDAD DEL INCIDENTE ATENDIENDO A SU IMPACTO Y URGENCIA Y TENIENDO EN CUENTA:**

- LOS COSTES POTENCIALES QUE SE PRODUCIRÍAN SI NO SE RESUELVE EL INCIDENTE.
- EL DAÑO QUE PUEDE CAUSAR A LOS DISTINTOS MIEMBROS DE LA ORGANIZACIÓN Y LOS COSTES IMPLÍCITOS QUE SE PUEDEN PRODUCIR POR UNA INTERRUPCIÓN DE LA COMUNICACIÓN ENTRE ELLOS.
- LAS IMPLICACIONES LEGALES QUE PUEDE SUPONER.

# 3. CATEGORIZACIÓN DE LOS INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES EN FUNCIÓN DE SU IMPACTO POTENCIAL

## CATEGORIZACIÓN DE LOS INCIDENTES

LA GESTIÓN DE INCIDENTES TENIENDO EN CUENTA SU **NIVEL DE IMPACTO** CLASIFICA LOS INCIDENTES DEL SIGUIENTE MODO:

- **INCIDENTES DE ALTO IMPACTO**
- **INCIDENTES DE IMPACTO MEDIO**
- **INCIDENTES DE IMPACTO BAJO**

# 3. CATEGORIZACIÓN DE LOS INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES EN FUNCIÓN DE SU IMPACTO POTENCIAL

## CATEGORIZACIÓN DE LOS INCIDENTES

### INCIDENTES DE ALTO IMPACTO

TIENEN UN **IMPACTO MUY ELEVADO** SOBRE LA ACTIVIDAD DE LA ORGANIZACIÓN Y EL SERVICIO QUE OFRECE.

### INCIDENTES DE IMPACTO MEDIO

TIENEN UN **IMPACTO SIGNIFICATIVO** SOBRE LA ACTIVIDAD DE LA ORGANIZACIÓN. TAMBIÉN ESTÁN EN ESTE NIVEL LOS INCIDENTES QUE TIENEN UN IMPACTO POTENCIALMENTE ELEVADO SOBRE LA ORGANIZACIÓN Y SU ACTIVIDAD.

### INCIDENTES DE IMPACTO BAJO

NO LLEGAN A TENER UN IMPACTO SIGNIFICATIVO SOBRE LA ORGANIZACIÓN, SU ACTIVIDAD Y SUS SERVICIOS. ESTOS INCIDENTES SIMPLEMENTE TIENEN EL POTENCIAL DE TENER IMPACTO SIGNIFICATIVO.

# CONTENIDOS

1. INTRODUCCIÓN
2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES
3. CATEGORIZACIÓN DE LOS INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES EN FUNCIÓN DE SU IMPACTO POTENCIAL
4. **CRITERIOS PARA LA DETERMINACIÓN DE LAS EVIDENCIAS OBJETIVAS EN LAS QUE SE SOPORTARÁ LA GESTIÓN DEL INCIDENTE**
5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES
6. GUÍA PARA LA CLASIFICACIÓN Y ANÁLISIS INICIAL DEL INTENTO DE INTRUSIÓN O INFECCIÓN CONTEMPLANDO EL IMPACTO PREVISIBLE DEL MISMO
7. ESTABLECIMIENTO DEL NIVEL DE INTERVENCIÓN REQUERIDO EN FUNCIÓN DEL IMPACTO PREVISIBLE
8. GUÍA PARA LA INVESTIGACIÓN Y DIAGNÓSTICO DEL INCIDENTE DE INTENTO DE INTRUSIÓN O INFECCIONES
9. ESTABLECIMIENTO DEL PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE LOS SISTEMAS TRAS UN INCIDENTE DERIVADO DE UN INTENTO DE INTRUSIÓN O INFECCIÓN
10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE
11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE Y LOS REGISTROS NECESARIOS PARA DOCUMENTAR EL HISTÓRICO DEL INCIDENTE

# 4. CRITERIOS PARA LA DETERMINACIÓN DE LAS EVIDENCIAS OBJETIVAS EN LAS QUE SE SOPORTARÁ LA GESTIÓN DEL INCIDENTE

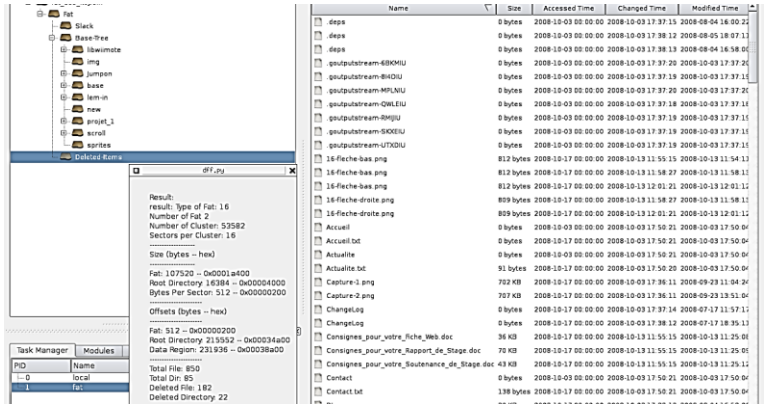
PARA COMBATIR CORRECTAMENTE EL INCIDENTE PREVIAMENTE **HAY QUE LLEVAR A CABO UN PROCESO DE IDENTIFICACIÓN QUE INCLUYE LA BÚSQUEDA Y DETERMINACIÓN DE LAS EVIDENCIAS OBJETIVAS**.

CON ESTAS EVIDENCIAS LA DECISIÓN DE LAS MEDIDAS A TOMAR PUEDE SER MÁS PRECISA Y EFECTIVA Y, ADEMÁS, CON LA INFORMACIÓN OBTENIDA SE PUEDEN ESTABLECER MEDIDAS PREVENTIVAS CON LAS QUE SE EVITARÁ QUE ESE INCIDENTE SE VUELVA A PRODUCIR.

# 4. CRITERIOS PARA LA DETERMINACIÓN DE LAS EVIDENCIAS OBJETIVAS EN LAS QUE SE SOPORTARÁ LA GESTIÓN DEL INCIDENTE

LA RECOLECCIÓN DE EVIDENCIAS DEBE **REALIZARSE DE UN MODO MUY METÓDICO PARA EVITAR BORRAR *HUELLAS* DEL INCIDENTE** QUE DIFICULTEN SU IDENTIFICACIÓN.

LAS HERRAMIENTAS QUE SE UTILIZAN EN **ANÁLISIS FORENSE** ESTÁN MUY AVANZADAS Y PERMITEN CONOCER EXACTAMENTE LOS MECANISMOS QUE HA UTILIZADO EL INTRUSO PARA ACCEDER AL SISTEMA Y LOS CAMBIOS QUE SE HAN PRODUCIDO.



# 4. CRITERIOS PARA LA DETERMINACIÓN DE LAS EVIDENCIAS OBJETIVAS EN LAS QUE SE SOPORTARÁ LA GESTIÓN DEL INCIDENTE

UNA RECOMENDACIÓN IMPORTANTE ES LA **CREACIÓN DE UNA COPIA DE SEGURIDAD** COMO HERRAMIENTA BÁSICA PARA LA RESPUESTA A INCIDENTES:

HAY QUE TENER EN CUENTA QUE **NUMEROSAS INTRUSIONES PUEDEN MODIFICAR LAS APLICACIONES Y UTILIDADES DE SEGURIDAD** QUE INCLUYEN LOS SISTEMAS OPERATIVOS Y AL REALIZAR LA RECOPILACIÓN DE EVIDENCIAS, SI HA HABIDO MODIFICACIONES QUE SEAN DIFÍCILES DE PERCIBIR, SERÁ COMPLICADO DETECTARLAS.

# 4. CRITERIOS PARA LA DETERMINACIÓN DE LAS EVIDENCIAS OBJETIVAS EN LAS QUE SE SOPORTARÁ LA GESTIÓN DEL INCIDENTE

EN ESTA COPIA SE RECOMIENDA QUE SE INCLUYAN LAS SIGUIENTES **TAREAS**:

- ENUMERAR LOS PUERTOS TCP Y UDP ABIERTOS Y LAS APLICACIONES QUE LLEVAN ASOCIADAS CADA UNO DE ELLOS.
- INTERPRETACIÓN DE LOS COMANDOS EN MODO CONSOLA.
- ENUMERACIÓN DE LOS USUARIOS QUE SE CONECTAN AL SISTEMA TANTO EN LOCAL COMO EN MODO REMOTO.
- OBTENCIÓN DE LA HORA Y FECHA DEL SISTEMA OPERATIVO.
- ELABORACIÓN DE UNA LISTA DE LOS PROCESOS ACTIVOS, LOS RECURSOS UTILIZADOS Y LOS USUARIOS O APLICACIONES QUE LOS INICIARON.
- LISTAR LAS DIRECCIONES IP.
- BÚSQUEDA DE LOS FICHEROS OCULTOS O ELIMINADOS.
- VISUALIZAR LOS DISTINTOS LOGS Y REGISTROS DEL SISTEMA.
- LECTURA, COPIA Y ESCRITURA A TRAVÉS DE LA RED.
- REALIZACIÓN DE COPIAS DE DISCOS DUROS Y PARTICIONES.
- ANÁLISIS DEL TRÁFICO DE DATOS DE LA RED.
- VISUALIZACIÓN DE LA CONFIGURACIÓN DE SEGURIDAD DEL SISTEMA.

# 4. CRITERIOS PARA LA DETERMINACIÓN DE LAS EVIDENCIAS OBJETIVAS EN LAS QUE SE SOPORTARÁ LA GESTIÓN DEL INCIDENTE

EL SIGUIENTE PASO CONSISTE EN LA **BÚSQUEDA REAL DE LOS INDICIOS DEL ATAQUE**.

EL PRIMER SITIO A BUSCAR ES **EN LOS EQUIPOS QUE SE CONSIDERAN MÁS COMPROMETIDOS**, PERO NO HAY QUE OLVIDAR QUE LOS ATACANTES HAN PODIDO ELIMINAR REGISTROS LOCALES EN ESTOS EQUIPOS Y TAMBIÉN EN EQUIPOS O DISPOSITIVOS PRÓXIMOS A ELLOS

HAY QUE BUSCAR INDICIOS TAMBIÉN EN **ESCANEO DE PUERTOS Y EN LA BÚSQUEDA DE TRÁFICO INUSUAL EN LOS CORTAFUEGOS Y ROUTERS** DE LA RED.

# 4. CRITERIOS PARA LA DETERMINACIÓN DE LAS EVIDENCIAS OBJETIVAS EN LAS QUE SE SOPORTARÁ LA GESTIÓN DEL INCIDENTE

**ES RECOMENDABLE CONOCER LOS PROCESOS QUE SE EJECUTAN EN ESE MOMENTO** EN CADA UNO DE ELLOS PARA BUSCAR CONSUMOS EXCESIVOS DE RECURSOS, UBICACIONES DE ARCHIVOS POCO FRECUENTES, UTILIZACIÓN DE PUERTOS NO HABITUALES, ETC.

SI SE ENCUENTRAN INDICIOS DE POSIBLES INTRUSIONES EL SIGUIENTE PASO ES **OBTENER LOS ARCHIVOS DE REGISTRO DEL SISTEMA Y LOGS** PARA DETECTAR ACCESOS NO AUTORIZADOS, CONEXIONES FALLIDAS, AVISOS SOBRE FALLOS DE INSTALACIÓN, ETC.

LA OBSERVACIÓN DE LOS ARCHIVOS DE REGISTRO VARÍA SEGÚN EL SISTEMA OPERATIVO QUE SE UTILIZA.

# 4. CRITERIOS PARA LA DETERMINACIÓN DE LAS EVIDENCIAS OBJETIVAS EN LAS QUE SE SOPORTARÁ LA GESTIÓN DEL INCIDENTE

## CRITERIOS PARA LA RECOLECCIÓN DE EVIDENCIAS

PARA LLEVAR A CABO LA RECOLECCIÓN DE EVIDENCIAS SE RECOMIENDA TENER EN CUENTA UNA SERIE DE **CRITERIOS DE SENSORES**:

- **BASADOS EN EQUIPO O HOST BASED SENSORS**
- **BASADOS EN APLICACIÓN O APPLICATION BASED SENSORS**
- **BASADOS EN RED O NETWORK BASED SENSORS**

# 4. CRITERIOS PARA LA DETERMINACIÓN DE LAS EVIDENCIAS OBJETIVAS EN LAS QUE SE SOPORTARÁ LA GESTIÓN DEL INCIDENTE

## CRITERIOS PARA LA RECOLECCIÓN DE EVIDENCIAS

### BASADOS EN EQUIPO O HOST BASED SENSORS

**SE ENCARGAN DE OBTENER INFORMACIÓN DE LOS EVENTOS A NIVEL DEL SISTEMA OPERATIVO** (INTENTOS DE CONEXIÓN, ACCESOS AL SISTEMA OPERATIVO, ETC.).

COMO **VENTAJA** ES IMPORTANTE DESTACAR QUE **LA INFORMACIÓN QUE RECOGEN ES DE CALIDAD.** ADEMÁS, SE CONFIGURAN CON FACILIDAD Y SUMINISTRAN INFORMACIÓN CON ALTOS NIVELES DE PRECISIÓN.

COMO **INCONVENIENTE** CABE DECIR QUE ESTOS SENSORES **PUEDEN AFECTAR CONSIDERABLEMENTE A LA EFICIENCIA DEL SISTEMA** EN EL QUE SE EJECUTAN AL CONSUMIR UN ELEVADO NIVEL DE RECURSOS.

# 4. CRITERIOS PARA LA DETERMINACIÓN DE LAS EVIDENCIAS OBJETIVAS EN LAS QUE SE SOPORTARÁ LA GESTIÓN DEL INCIDENTE

## CRITERIOS PARA LA RECOLECCIÓN DE EVIDENCIAS

### BASADOS EN APLICACIÓN O APPLICATION BASED SENSORS

LA FUNCIÓN PRINCIPAL DE ESTOS SENSORES ES **OBTENER INFORMACIÓN DE LAS APLICACIONES QUE SE EJECUTAN EN EL SISTEMA**: SON UNA PECULIARIDAD DE LOS SENSORES BASADOS EN EQUIPO.

LAS **VENTAJAS E INCONVENIENTES** SON LOS MISMOS QUE EN LOS SENSORES BASADOS EN EQUIPOS: OBTIENEN INFORMACIÓN DE CALIDAD, SON FÁCILES DE CONFIGURAR Y, POR EL CONTRARIO, TIENEN UN CONSUMO INTENSIVO DE LOS RECURSOS DEL SISTEMA.

# 4. CRITERIOS PARA LA DETERMINACIÓN DE LAS EVIDENCIAS OBJETIVAS EN LAS QUE SE SOPORTARÁ LA GESTIÓN DEL INCIDENTE

## CRITERIOS PARA LA RECOLECCIÓN DE EVIDENCIAS

### BASADOS EN RED O NETWORK BASED SENSORS

**RECOLECTAN INFORMACIÓN DE LOS EVENTOS QUE SUCEDEN EN EL TRÁFICO DE DATOS DE LA RED**. PERMITEN TRABAJAR Y OBTENER INFORMACIÓN SIN AFECTAR A LOS RECURSOS DEL EQUIPO NI A LA INFRAESTRUCTURA DE RED.

SU NIVEL DE SEGURIDAD ES MÁS ELEVADO QUE LOS DEMÁS CRITERIOS, TIENEN MÁS NIVEL DE RESISTENCIA ANTE POSIBLES ATAQUES.

LA **VENTAJA PRINCIPAL** ES LA **CAPACIDAD DE OBTENER INFORMACIÓN A NIVEL DE RED** QUE LOS OTROS SENSORES NO OFRECEN.

# 4. CRITERIOS PARA LA DETERMINACIÓN DE LAS EVIDENCIAS OBJETIVAS EN LAS QUE SE SOPORTARÁ LA GESTIÓN DEL INCIDENTE

## CRITERIOS PARA LA RECOLECCIÓN DE EVIDENCIAS

LA DECISIÓN DE QUÉ CRITERIO ES MEJOR HA SIDO AMPLIAMENTE DEBATIDA EN ESTOS ÚLTIMOS AÑOS, YA QUE CADA CRITERIO OFRECE PRESTACIONES QUE LOS DEMÁS NO FACILITAN.

DEPENDIENDO DEL TIPO DE INFORMACIÓN QUE SE PRETENDA OBTENER (A NIVEL DE SISTEMA, A NIVEL DE APLICACIÓN O A NIVEL DE RED) DEBERÁ DECIDIRSE LA UTILIZACIÓN DE UNOS CRITERIOS U OTROS.

ANTE LA DUDA, **LOS IDS/IPS OFRECEN SOLUCIONES HÍBRIDAS QUE UNIFICAN LAS TRES OPCIONES** (SUMINISTRANDO INFORMACIÓN DE LOS EQUIPOS PROTEGIDOS Y DE LOS DATOS QUE CIRCULAN ENTRE ELLOS) Y FACILITAN INFORMACIÓN MÁS COMPLETA Y EXTENSA.

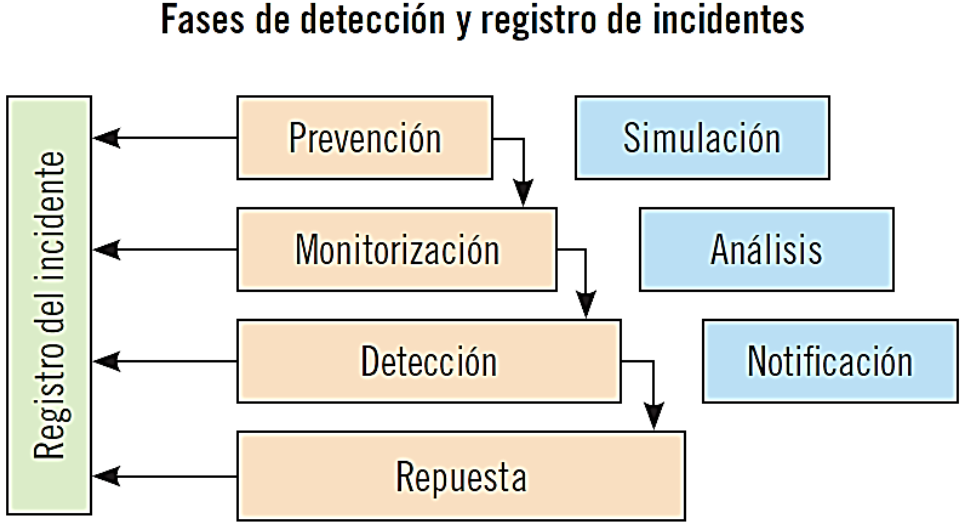
# CONTENIDOS

1. INTRODUCCIÓN
2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES
3. CATEGORIZACIÓN DE LOS INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES EN FUNCIÓN DE SU IMPACTO POTENCIAL
4. CRITERIOS PARA LA DETERMINACIÓN DE LAS EVIDENCIAS OBJETIVAS EN LAS QUE SE SOPORTARÁ LA GESTIÓN DEL INCIDENTE
5. **ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES**
6. GUÍA PARA LA CLASIFICACIÓN Y ANÁLISIS INICIAL DEL INTENTO DE INTRUSIÓN O INFECCIÓN CONTEMPLANDO EL IMPACTO PREVISIBLE DEL MISMO
7. ESTABLECIMIENTO DEL NIVEL DE INTERVENCIÓN REQUERIDO EN FUNCIÓN DEL IMPACTO PREVISIBLE
8. GUÍA PARA LA INVESTIGACIÓN Y DIAGNÓSTICO DEL INCIDENTE DE INTENTO DE INTRUSIÓN O INFECCIONES
9. ESTABLECIMIENTO DEL PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE LOS SISTEMAS TRAS UN INCIDENTE DERIVADO DE UN INTENTO DE INTRUSIÓN O INFECCIÓN
10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE
11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE Y LOS REGISTROS NECESARIOS PARA DOCUMENTAR EL HISTÓRICO DEL INCIDENTE

# 5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES

UNA VEZ DETECTADO EL INCIDENTE, YA SERÁN LOS RESPONSABLES DESIGNADOS LOS QUE DEBEN ENCARGARSE DE **TOMAR MEDIDAS DE RESPUESTA Y DE REGISTRAR TODOS LOS EVENTOS PRODUCIDOS Y ACCIONES EJECUTADAS**.

LAS **FASES DE DETECCIÓN Y REGISTRO DE INCIDENTES** SE PUEDEN OBSERVAR EN LA SIGUIENTE IMAGEN:



# 5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES

## FASE DE PREVENCIÓN DE INCIDENTES

LOS SISTEMAS DE PREVENCIÓN DE INTRUSIONES SON HERRAMIENTAS FUNDAMENTALES Y EFICACES ENCARGADAS DE EVITAR QUE CUALQUIER TIPO DE INTRUSIÓN ACCEDA A LOS EQUIPOS Y DISPOSITIVOS DE UNA RED.

ESTAS HERRAMIENTAS REALIZAN SIMULACIONES CON EL TRÁFICO DE LA RED PARA IDENTIFICAR ACTIVIDADES QUE PUEDEN LLEGAR A SER INTRUSIONES REALES. SUS TIPOLOGÍAS SON:

- **DETECCIÓN BASADA EN FIRMAS**
- **DETECCIÓN BASADA EN POLÍTICAS**
- **DETECCIÓN BASADA EN ANOMALÍAS**
- **DETECCIÓN HONEY POT O JARRA DE MIEL**

# 5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES

## FASE DE PREVENCIÓN DE INCIDENTES

### DETECCIÓN BASADA EN FIRMAS

COMPARA LA ACTIVIDAD DE LA RED EN BÚSQUEDA DE POSIBLES INTRUSIONES REGISTRADAS EN SU BASE DE DATOS.

### DETECCIÓN BASADA EN POLÍTICAS

DETECTA LAS INTRUSIONES ATENDIENDO A LAS POLÍTICAS DE SEGURIDAD MARCADAS POR LA ORGANIZACIÓN.

# 5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES

## FASE DE PREVENCIÓN DE INCIDENTES

### DETECCIÓN BASADA EN ANOMALÍAS

COMPARA LA ACTIVIDAD DE LA RED CON ACTIVIDADES INUSUALES PARA ANALIZARLAS Y DETECTAR POSIBLES ANOMALÍAS E INTRUSIONES.

### DETECCIÓN HONEY POT O JARRA DE MIEL

PREVIENE LAS INTRUSIONES USANDO UN EQUIPO CONFIGURADO ESPECÍFICAMENTE PARA ATRAER INTRUSIONES Y CONSEGUIR DESVIAR SU ATENCIÓN DE LOS EQUIPOS QUE CONTIENEN LA INFORMACIÓN IMPORTANTE.

# 5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES

## FASE DE MONITORIZACIÓN DE INCIDENTES

EN ESTA FASE SE MONITORIZA EL TRÁFICO DE RED DEL SISTEMA CON LA FINALIDAD DE PODER ANALIZARLO Y COMPROBAR QUE TODO FUNCIONA COMO SE ESPERA.

**SI SE DETECTA ALGÚN TIPO DE ACTIVIDAD INUSUAL O SOSPECHOSA HAY QUE PROCEDER A SU MONITORIZACIÓN**.

CON ESTO SE AYUDA A LA DETECCIÓN DE INTENTOS DE INTRUSIÓN Y PERMITE EJECUTAR MEDIDAS DE RESPUESTA MÁS RÁPIDAMENTE.

# 5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES

## FASE DE MONITORIZACIÓN DE INCIDENTES

PARA QUE LA MONITORIZACIÓN SEA MÁS EFECTIVA **SE RECOMIENDA CONFIGURAR UN SISTEMA DE ALERTAS** QUE AVISE **MEDIANTE MENSAJES EN PANTALLA, ENVÍO DE CORREOS ELECTRÓNICOS** A LOS RESPONSABLES U OTROS MÉTODOS CUANDO SE DETECTE CUALQUIER TIPO DE ACTIVIDAD SOSPECHOSA COMO PROCESADORES SOBRECARGADOS, CONSUMO EXCESIVO DE RECURSOS, ETC.

CON LA UTILIZACIÓN DE ESTOS SISTEMAS DE ALERTAS **SE CONSIGUE UNA REACCIÓN MÁS RÁPIDA** Y, POR TANTO, UNAS **MEDIDAS MÁS EFICACES** QUE CONSIGAN CONTENER Y ELIMINAR LA INTRUSIÓN CON MAYOR RAPIDEZ Y MENOR CANTIDAD DE DAÑOS ORIGINADOS.

# 5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES

## FASE DE DETECCIÓN DE LA INTRUSIÓN

CON LA MONITORIZACIÓN DEL TRÁFICO DE RED Y DE LOS PROCESOS QUE SE ESTÁN EJECUTANDO YA HABRÁ INDICIOS SUFICIENTES QUE DETERMINARÁN SI LA ACTIVIDAD SOSPECHOSA ES REALMENTE UNA INTRUSIÓN O NO.

EN ESTE CASO LA **CONFIGURACIÓN DE LOS IDS/IPS DEBE REALIZARSE POR TÉCNICOS EXPERIMENTADOS** QUE PRUEBEN LA SENSIBILIDAD DE LA HERRAMIENTA Y ENCUENTREN EL PUNTO DE EQUILIBRIO ENTRE LA DETECCIÓN DE AMENAZAS REALES Y LA DETECCIÓN DE FALSAS ALARMAS.

# 5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES

## FASE DE DETECCIÓN DE LA INTRUSIÓN

UNA **MAYOR SENSIBILIDAD** EVITA QUE ALGUNAS INTRUSIONES PASEN DESAPERCIBIDAS, PERO TAMBIÉN DETECTA COMO POSIBLE INTRUSIÓN UN **MAYOR NÚMERO DE FALSAS ALARMAS.**

UNA CONFIGURACIÓN DE **POCA SENSIBILIDAD** DETECTARÁ **POCAS** INTRUSIONES QUE SEAN **FALSAS ALARMAS**, PERO, SIN EMBARGO**, DEJARÁ DE DETECTAR OTRAS INTRUSIONES REALES** QUE PUEDEN TENER GRAVES EFECTOS SOBRE EL SISTEMA AL QUE ACCEDAN.

# 5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES

## FASE DE RESPUESTA

LOS **SISTEMAS IDS**, EN GENERAL, NO PUEDEN COMBATIR Y ELIMINAR LA AMENAZA, SIMPLEMENTE SE LIMITAN A SU **DETECCIÓN** Y A LA **GENERACIÓN DE ALERTAS** QUE PERMITAN A LOS RESPONSABLES LA TOMA DE MEDIDAS REACTIVAS.

SIN EMBARGO, LOS **SISTEMAS IPS** MÁS SOFISTICADOS QUE INCLUYEN **MEDIDAS DE CONTINGENCIA O CUARENTENA** PARA EVITAR DAÑOS MAYORES ANTE LA DETECCIÓN DE INTRUSIONES: **CIERRE DE PUERTOS, BLOQUEO DE TRÁFICO DE RED, ETC.**

# 5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES

## FASE DE RESPUESTA

LAS RESPUESTAS QUE PUEDEN GENERAR LOS SISTEMAS IDS SE PUEDEN CLASIFICAR EN:

- **RESPUESTAS PASIVAS:** NOTIFICACIÓN A LOS RESPONSABLES DE SEGURIDAD DE LA INTRUSIÓN O ATAQUE DETECTADO.
- **RESPUESTAS ACTIVAS:** REALIZACIÓN DE ACCIONES AUTOMÁTICAS CONFIGURADAS ESPECÍFICAMENTE PARA QUE OBTENGAN MÁS INFORMACIÓN SOBRE EL POSIBLE ATAQUE.

# 5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES

## REGISTRO DEL INCIDENTE

ESTA FASE DEL PROCESO DE GESTIÓN DE INCIDENTES **SE DEBE PRODUCIR A LO LARGO DE TODO EL INCIDENTE,** DESDE LA DETECCIÓN PREVIA DE POSIBLES INDICIOS DE INTRUSIÓN HASTA EL MOMENTO EN EL QUE SE RESTAURA LA SITUACIÓN INCLUYENDO EL MOMENTO ANTERIOR DE LA ENTRADA DE LA INTRUSIÓN.

CONSISTE EN LA **GENERACIÓN DE UN ARCHIVO DE REGISTRO EN EL QUE SE VAYAN ALMACENANDO TODOS LOS DETALLES DETECTADOS DE LA INTRUSIÓN Y TODAS LAS ACCIONES TOMADAS A CABO PARA SU CONTENCIÓN, ERRADICACIÓN Y RESTAURACIÓN DEL SISTEMA.**

# 5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES

## REGISTRO DEL INCIDENTE

EL REGISTRO DE LOS INCIDENTES **ES UNA HERRAMIENTA MUY ÚTIL EN EL MOMENTO DE REALIZAR UN ANÁLISIS FORENSE DE LA INTRUSIÓN**, YA QUE FACILITA INFORMACIÓN SOBRE TODO LO QUE HA ESTADO OCURRIENDO EN EL DESARROLLO DE LA MISMA JUNTO CON EL ORDEN CRONOLÓGICO DE LAS ACCIONES TOMADAS.

CON UN ANÁLISIS PROFUNDO DE LOS ARCHIVOS DE REGISTRO LOS ANALISTAS FORENSES PUEDEN CONOCER CON DETALLE CÓMO Y POR DÓNDE HA CONSEGUIDO ACCEDER LA INTRUSIÓN Y QUÉ ES LO QUE HA PODIDO FALLAR EN SU DETECCIÓN Y PREVENCIÓN.

# 5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES

## REGISTRO DEL INCIDENTE

DE ESTE MODO Y **MEDIANTE EL ANÁLISIS FORENSE DE LA INFORMACIÓN APORTADA POR LOS ARCHIVOS DE REGISTRO SE PUEDE REALIZAR UN PROCESO DE APRENDIZAJE** QUE CULMINE EN EL DISEÑO DE NUEVAS MEDIDAS QUE EVITEN QUE INCIDENTES FUTUROS PARECIDOS A LOS YA SUCEDIDOS NO PUEDAN VOLVER A ACCEDER A LOS SISTEMAS DE LA ORGANIZACIÓN.

# CONTENIDOS

1. INTRODUCCIÓN
2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES
3. CATEGORIZACIÓN DE LOS INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES EN FUNCIÓN DE SU IMPACTO POTENCIAL
4. CRITERIOS PARA LA DETERMINACIÓN DE LAS EVIDENCIAS OBJETIVAS EN LAS QUE SE SOPORTARÁ LA GESTIÓN DEL INCIDENTE
5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES
6. **GUÍA PARA LA CLASIFICACIÓN Y ANÁLISIS INICIAL DEL INTENTO DE INTRUSIÓN O INFECCIÓN CONTEMPLANDO EL IMPACTO PREVISIBLE DEL MISMO**
7. ESTABLECIMIENTO DEL NIVEL DE INTERVENCIÓN REQUERIDO EN FUNCIÓN DEL IMPACTO PREVISIBLE
8. GUÍA PARA LA INVESTIGACIÓN Y DIAGNÓSTICO DEL INCIDENTE DE INTENTO DE INTRUSIÓN O INFECCIONES
9. ESTABLECIMIENTO DEL PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE LOS SISTEMAS TRAS UN INCIDENTE DERIVADO DE UN INTENTO DE INTRUSIÓN O INFECCIÓN
10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE
11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE Y LOS REGISTROS NECESARIOS PARA DOCUMENTAR EL HISTÓRICO DEL INCIDENTE

# 6. GUÍA PARA LA CLASIFICACIÓN Y ANÁLISIS INICIAL DEL INTENTO DE INTRUSIÓN O INFECCIÓN CONTEMPLANDO EL IMPACTO PREVISIBLE DEL MISMO

PARA CLASIFICAR Y LLEVAR A CABO UN ANÁLISIS INICIAL DEL INTENTO DE INTRUSIÓN HAY QUE TENER EN CUENTA EL IMPACTO QUE SE PREVÉ QUE VA A HABER.

SEGÚN EL IMPACTO QUE PUEDA PROVOCAR SE DEBERÁN TOMAR MEDIDAS DE URGENCIA O SE PODRÁ DEMORAR SU ELIMINACIÓN ANTE OTRAS PRIORIDADES.

SE PUEDEN CLASIFICAR POR **VARIOS CRITERIOS**:

- **ATENDIENDO A SU NATURALEZA**
- **ATENDIENDO A SUS VÍAS DE ACCESO**
- **ATENDIENDO A SU IMPACTO**

# 6. GUÍA PARA LA CLASIFICACIÓN Y ANÁLISIS INICIAL DEL INTENTO DE INTRUSIÓN O INFECCIÓN CONTEMPLANDO EL IMPACTO PREVISIBLE DEL MISMO

## INTENTOS DE INTRUSIÓN ATENDIENDO A SU NATURALEZA

- **INTRUSIONES DE USO ERRÓNEO:** INTRUSIONES *DISEÑADAS PARA ATACAR LOS PUNTOS DÉBILES DE UN SISTEMA.* SE PUEDEN DETECTAR CON LA OBSERVACIÓN DE ACCIONES SUCEDIDAS EN DICHO SISTEMA.
- **INTRUSIONES DE ANOMALÍA:** INTRUSIONES QUE *ATACAN DESVIANDO LAS ACCIONES DE UN SISTEMA DE SU UTILIZACIÓN HABITUAL.* SE PUEDEN DETECTAR GUARDANDO LOS PERFILES DEL SISTEMA EN SITUACIONES NORMALES Y COMPARÁNDOLAS PERIÓDICAMENTE PARA DETECTAR ALTERACIONES Y ANOMALÍAS IMPORTANTES.

# 6. GUÍA PARA LA CLASIFICACIÓN Y ANÁLISIS INICIAL DEL INTENTO DE INTRUSIÓN O INFECCIÓN CONTEMPLANDO EL IMPACTO PREVISIBLE DEL MISMO

## INTENTOS DE INTRUSIÓN ATENDIENDO A SUS VÍAS DE ACCESO

- **INTRUSIÓN FÍSICA:** EL INTRUSO *ACCEDE AL EQUIPO A TRAVÉS DE UN MEDIO FÍSICO* (POR EJEMPLO, CON EL TECLADO).
- **INTRUSIÓN DEL SISTEMA:** EL INTRUSO *UTILIZA UNA CUENTA DE USUARIO DEL SISTEMA* CON POCOS PRIVILEGIOS SOBRE LA QUE ACTUARÁ PARA QUE SE LE ASIGNEN OTROS PRIVILEGIOS MÁS SIGNIFICATIVOS Y PODER ATACAR EN CONSECUENCIA.
- **INTRUSIÓN ALEJADA:** EL INTRUSO *ACCEDE AL SISTEMA CON ACCESO REMOTO* A TRAVÉS DE LA RED.

# 6. GUÍA PARA LA CLASIFICACIÓN Y ANÁLISIS INICIAL DEL INTENTO DE INTRUSIÓN O INFECCIÓN CONTEMPLANDO EL IMPACTO PREVISIBLE DEL MISMO

## INTENTOS DE INTRUSIÓN ATENDIENDO A 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.

SE PUEDEN DISTINGUIR VARIOS TIPOS DE INTRUSIONES:

- **INTENTOS DE ENTRADA**
- **ATAQUES ENMASCARADOS**
- **PENETRACIONES EN EL SISTEMA DE CONTROL**
- **DENEGACIÓN DE SERVICIO**
- **USO MALICIOSO**

# 6. GUÍA PARA LA CLASIFICACIÓN Y ANÁLISIS INICIAL DEL INTENTO DE INTRUSIÓN O INFECCIÓN CONTEMPLANDO EL IMPACTO PREVISIBLE DEL MISMO

## INTENTOS DE INTRUSIÓN ATENDIENDO A 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. GUÍA PARA LA CLASIFICACIÓN Y ANÁLISIS INICIAL DEL INTENTO DE INTRUSIÓN O INFECCIÓN CONTEMPLANDO EL IMPACTO PREVISIBLE DEL MISMO

## INTENTOS DE INTRUSIÓN ATENDIENDO A SU IMPACTO

### ATAQUES ENMASCARADOS

EL INTRUSO UTILIZA *USUARIOS YA REGISTRADOS A TRAVÉS DE LOS CUALES INTENTAR ATACAR*.

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. ESO SÍ, SI ACCEDE A TRAVÉS DEL ADMINISTRADOR LOS EFECTOS PUEDEN SER NEFASTOS.

COMO NO ES SEGURO Y EL DAÑO EN ESTE CASO SE CONSIDERA POTENCIALMENTE SIGNIFICATIVO, EL **IMPACTO** SERÁ **MEDIO**.

# 6. GUÍA PARA LA CLASIFICACIÓN Y ANÁLISIS INICIAL DEL INTENTO DE INTRUSIÓN O INFECCIÓN CONTEMPLANDO EL IMPACTO PREVISIBLE DEL MISMO

## INTENTOS DE INTRUSIÓN ATENDIENDO A SU IMPACTO

### PENETRACIONES EN EL SISTEMA DE CONTROL

LOS INTRUSOS INTENTAN *ACCEDER A LAS HERRAMIENTAS DE CONTROL DEL SISTEMA CON EL FIN DE ALTERARLAS*. 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 CONTROLAN TODOS LOS DEMÁS PROCESOS, USUARIOS, RENDIMIENTOS Y DEMÁS CARACTERÍSTICAS Y CONTENIDOS DEL EQUIPO AL QUE SE ESTÁ ADMINISTRANDO. SE SUELEN DETECTAR MEDIANTE LA OBSERVACIÓN COMPORTAMIENTOS ESPECIALES FUERA DE LO HABITUAL.

# 6. GUÍA PARA LA CLASIFICACIÓN Y ANÁLISIS INICIAL DEL INTENTO DE INTRUSIÓN O INFECCIÓN CONTEMPLANDO EL IMPACTO PREVISIBLE DEL MISMO

## INTENTOS DE INTRUSIÓN ATENDIENDO A SU IMPACTO

### DENEGACIÓN DE SERVICIO

TIENEN COMO *OBJETIVO LIMITAR E INCLUSO IMPEDIR EL ACCESO A LOS RECURSOS Y SERVICIOS* DE UNA ORGANIZACIÓN.

SU **IMPACTO** ES **BAJO**, YA QUE, AUNQUE IMPIDE LA ACTIVIDAD HABITUAL DE UNA ORGANIZACIÓN, NO HAY ALTERACIÓN NI BORRADO DE DATOS.

SU **DETECCIÓN** ES **BASTANTE SIMPLE**, AUNQUE SU **PREVENCIÓN** ES **MÁS DIFICULTOSA.** LA DETECCIÓN DE LOS ATAQUES DE DENEGACIÓN DE SERVICIO SE PRODUCE AL OBSERVAR LA DIFICULTAD DE OFRECER LOS SERVICIOS A LOS USUARIOS POR PARTE DE LA ORGANIZACIÓN.

# 6. GUÍA PARA LA CLASIFICACIÓN Y ANÁLISIS INICIAL DEL INTENTO DE INTRUSIÓN O INFECCIÓN CONTEMPLANDO EL IMPACTO PREVISIBLE DEL MISMO

## INTENTOS DE INTRUSIÓN ATENDIENDO A SU IMPACTO

### 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 UTILIZADO **EL IMPACTO SERÁ DISTINTO**: DESDE SATURACIÓN DE SERVIDORES, BORRADO DE DATOS, APARICIÓN DE VENTANAS MOLESTAS, OBSERVACIÓN DE ACTIVIDAD, ENVÍO DE SPAM, ETC.

ESTE TIPO DE INTRUSIONES, A PESAR DE SU GRAN VARIEDAD, **SE SUELE DETECTAR POR LOS MODELOS DE COMPORTAMIENTO ATÍPICO** DEL SISTEMA O DE ALGUNA APLICACIÓN O PROCESO CONCRETO.

# CONTENIDOS

1. INTRODUCCIÓN
2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES
3. CATEGORIZACIÓN DE LOS INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES EN FUNCIÓN DE SU IMPACTO POTENCIAL
4. CRITERIOS PARA LA DETERMINACIÓN DE LAS EVIDENCIAS OBJETIVAS EN LAS QUE SE SOPORTARÁ LA GESTIÓN DEL INCIDENTE
5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES
6. GUÍA PARA LA CLASIFICACIÓN Y ANÁLISIS INICIAL DEL INTENTO DE INTRUSIÓN O INFECCIÓN CONTEMPLANDO EL IMPACTO PREVISIBLE DEL MISMO
7. **ESTABLECIMIENTO DEL NIVEL DE INTERVENCIÓN REQUERIDO EN FUNCIÓN DEL IMPACTO PREVISIBLE**
8. GUÍA PARA LA INVESTIGACIÓN Y DIAGNÓSTICO DEL INCIDENTE DE INTENTO DE INTRUSIÓN O INFECCIONES
9. ESTABLECIMIENTO DEL PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE LOS SISTEMAS TRAS UN INCIDENTE DERIVADO DE UN INTENTO DE INTRUSIÓN O INFECCIÓN
10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE
11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE Y LOS REGISTROS NECESARIOS PARA DOCUMENTAR EL HISTÓRICO DEL INCIDENTE

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

## CLASIFICACIÓN DE LOS INCIDENTES SEGÚN SU NIVEL DE CRITICIDAD

**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.

LOS EFECTOS NEGATIVOS PRODUCIDOS O POTENCIALES Y LA CRITICIDAD DE LOS RECURSOS SON LOS QUE **DETERMINARÁN EL NIVEL DE CRITICIDAD DEL INCIDENTE ATENDIENDO A SU IMPACTO**.

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

## CLASIFICACIÓN DE LOS INCIDENTES SEGÚN SU NIVEL DE CRITICIDAD

EL **ENS CLASIFICA** LOS INCIDENTES SEGÚN SU CRITICIDAD **EN CINCO CATEGORÍAS** O NIVELES:

- **NIVEL DE CRITICIDAD CRÍTICO**
- **NIVEL DE CRITICIDAD MUY ALTO**
- **NIVEL DE CRITICIDAD ALTO**
- **NIVEL DE CRITICIDAD MEDIO**
- **NIVEL DE CRITICIDAD BAJO**

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

## 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**.

*LOS RECURSOS* AFECTADOS POR LAS INTRUSIONES *CONTIENEN INFORMACIÓN CRÍTICA Y ESPECIALMENTE RELEVANTE* PARA LA BUENA MARCHA DE LA ORGANIZACIÓN.

SUELEN AFECTAR A LOS SERVICIOS UTILIZADOS POR UN ELEVADO NÚMERO DE USUARIOS, A RECURSOS QUE AFECTAN SUSTANCIALMENTE A LA SEGURIDAD DEL SISTEMA Y DE LA RED E INCLUSO PROVOCAR PÉRDIDAS IRRECUPERABLES DE INFORMACIÓN CRÍTICA.

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

## CLASIFICACIÓN DE LOS INCIDENTES SEGÚN SU NIVEL DE CRITICIDAD

### 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.

*SUS EFECTOS* TAMBIÉN *AFECTAN* A LA INTEGRIDAD, DISPONIBILIDAD Y CONFIDENCIALIDAD DE *LOS DATOS CRÍTICOS* Y AMENAZAN A *UN NÚMERO LIMITADO DE SISTEMAS NO CRÍTICOS*.

A PESAR DE LA NO CRITICIDAD DE LOS SISTEMAS, SU CONTENCIÓN Y RESOLUCIÓN CONLLEVA UN TRABAJO LABORIOSO Y CONSIDERABLE PARA LOS RESPONSABLES DE SEGURIDAD.

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

## 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.**

SUELEN SER *INTRUSIONES A EQUIPOS Y SISTEMAS* MUY LIMITADOS (NORMALMENTE SOLO A UN EQUIPO) *QUE NO CONTIENEN INFORMACIÓN RELEVANTE*.

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

## 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.**

LAS ORGANIZACIONES DEBERÍAN ESTAR CAPACITADAS PARA COMBATIR INTRUSIONES DE ESTE NIVEL SIN NECESIDAD DE RECURRIR A AGENTES EXTERNOS.

**ES RECOMENDABLE LA ELABORACIÓN DE INFORMES PERIÓDICOS DE ESTAS INTRUSIONES** PARA LLEVAR UN CONTROL Y COMPROBAR LA EFECTIVIDAD DE LAS MEDIDAS DE PREVENCIÓN IMPLANTADAS.

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

## CLASIFICACIÓN DE LOS INCIDENTES SEGÚN SU NIVEL DE CRITICIDAD

### NIVEL 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.

**SE RECOMIENDA LA ELABORACIÓN PERIÓDICA DE INFORMES** QUE LAS CONTENGAN PARA LLEVAR UN CONTROL DE LA EFECTIVIDAD DE LAS MEDIDAS Y CONTROLES DE PREVENCIÓN.

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

## CLASIFICACIÓN DE LOS INCIDENTES SEGÚN SU NIVEL DE CRITICIDAD

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

## NIVEL DE INTERVENCIÓN EN FUNCIÓN DEL IMPACTO Y CRITICIDAD DE LA INTRUSIÓN

EN EL MOMENTO QUE SE CONFIRMA QUE EL INTENTO DE INTRUSIÓN ES REAL **ES DE VITAL IMPORTANCIA QUE EL TIEMPO DE REACCIÓN SEA EL ADECUADO, TENIENDO EN CUENTA SU NIVEL DE CRITICIDAD**.

LAS EMPRESAS Y ORGANIZACIONES DEBERÁN REGISTRAR Y GESTIONAR CADA INTRUSIÓN INDIVIDUALMENTE SEGÚN LOS RECURSOS AFECTADOS Y SU NIVEL DE IMPACTO

A **MAYOR CRITICIDAD** DE LOS RECURSOS Y MAYOR NIVEL, **MENOR** DEBERÁ SER **EL TIEMPO** PASADO **DESDE SU DETECCIÓN HASTA SU REGISTRO**.

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

## NIVEL DE INTERVENCIÓN EN FUNCIÓN DEL IMPACTO Y CRITICIDAD DE LA INTRUSIÓN

CONCRETAMENTE Y TENIENDO EN CUENTA SU CRITICIDAD DEBERÁN REGISTRARSE LAS INTRUSIONES SEGÚN ESTAS PAUTAS:

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

## NIVEL DE INTERVENCIÓN EN FUNCIÓN DEL IMPACTO Y CRITICIDAD DE LA INTRUSIÓN

### INTERVENCIÓN PARA LA CONTENCIÓN Y ERRADICACIÓN DE LA INTRUSIÓN SEGÚN SU IMPACTO Y CRITICIDAD

**LAS ORGANIZACIONES**, IGUAL QUE CON EL REGISTRO Y NOTIFICACIÓN, **DEBEN ESTABLECER UN TIEMPO "OBJETIVO" MÁXIMO DE CONTENCIÓN Y ERRADICACIÓN DE LA INTRUSIÓN**.

DEBE EXISTIR UN PLAZO MÁXIMO PARA QUE LA INTRUSIÓN ESTÉ CONTROLADA (Y DEJE DE PRODUCIR DAÑOS SUSTANCIALES) Y PARA QUE LA INTRUSIÓN SE CIERRE DEFINITIVAMENTE, QUEDANDO RESTAURADA LA SITUACIÓN INICIAL DEL SISTEMA.

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

## NIVEL DE INTERVENCIÓN 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 |

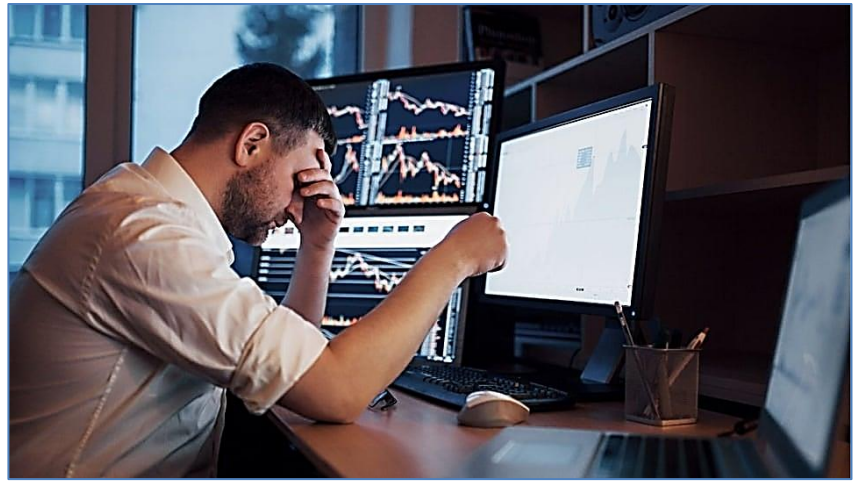
# CONTENIDOS

1. INTRODUCCIÓN
2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES
3. CATEGORIZACIÓN DE LOS INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES EN FUNCIÓN DE SU IMPACTO POTENCIAL
4. CRITERIOS PARA LA DETERMINACIÓN DE LAS EVIDENCIAS OBJETIVAS EN LAS QUE SE SOPORTARÁ LA GESTIÓN DEL INCIDENTE
5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES
6. GUÍA PARA LA CLASIFICACIÓN Y ANÁLISIS INICIAL DEL INTENTO DE INTRUSIÓN O INFECCIÓN CONTEMPLANDO EL IMPACTO PREVISIBLE DEL MISMO
7. ESTABLECIMIENTO DEL NIVEL DE INTERVENCIÓN REQUERIDO EN FUNCIÓN DEL IMPACTO PREVISIBLE
8. **GUÍA PARA LA INVESTIGACIÓN Y DIAGNÓSTICO DEL INCIDENTE DE INTENTO DE INTRUSIÓN O INFECCIONES**
9. ESTABLECIMIENTO DEL PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE LOS SISTEMAS TRAS UN INCIDENTE DERIVADO DE UN INTENTO DE INTRUSIÓN O INFECCIÓN
10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE
11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE Y LOS REGISTROS NECESARIOS PARA DOCUMENTAR EL HISTÓRICO DEL INCIDENTE

# 8. GUÍA PARA LA INVESTIGACIÓN Y DIAGNÓSTICO DEL INCIDENTE DE INTENTO DE INTRUSIÓN O INFECCIONES

CUANDO SE TIENEN SOSPECHAS DE QUE HA HABIDO ALGÚN ATAQUE O INTRUSIÓN EN EL SISTEMA HAY QUE **TENER EN CUENTA LOS SIGUIENTES ASPECTOS**:

- SI **ES REALMENTE UNA AMENAZA O ATAQUE**
- SI HA SIDO UN ATAQUE **CON ÉXITO O FALLIDO**
- LOS **DAÑOS PRODUCIDOS Y EL NIVEL DE COMPROMISO DEL SISTEMA AFECTADO** POR EL ATAQUE



# 8. GUÍA PARA LA INVESTIGACIÓN Y DIAGNÓSTICO DEL INCIDENTE DE INTENTO DE INTRUSIÓN O INFECCIONES

EN EL MOMENTO QUE SE TIENE CONFIRMADA LA PRESENCIA DE UN ATAQUE EN EL SISTEMA, ***EL PRIMER PASO A REALIZAR PARA INVESTIGAR SU PROCEDENCIA SERÁ COMPROBAR SI LOS USUARIOS QUE UTILIZAN EL SISTEMA*** *EN ESE MOMENTO PUEDEN SER SOSPECHOSOS.*

*EN CASO AFIRMATIVO,* ***COMPROBAR CUÁLES SON LOS SISTEMAS QUE SE ESTÁN EJECUTANDO Y QUIÉN LOS ESTÁ EJECUTANDO PARA TENER CONTROLADOS LOS USUARIOS QUE HAN PODIDO SER CAUSANTES DEL ATAQUE****.*

# 8. GUÍA PARA LA INVESTIGACIÓN Y DIAGNÓSTICO DEL INCIDENTE DE INTENTO DE INTRUSIÓN O INFECCIONES

PARA AVERIGUAR LOS USUARIOS QUE ESTÁN UTILIZANDO LAS APLICACIONES Y SISTEMAS EN EL MOMENTO DE LA INTRUSIÓN Y LOS DETALLES DE ESTOS **HABRÁ QUE SEGUIR UNA SERIE DE PASOS:**

- **VISUALIZAR LOS USUARIOS LOGUEADOS EN EL SISTEMA**
- **VISUALIZAR LOS PROCESOS ACTIVOS**

# 8. GUÍA PARA LA INVESTIGACIÓN Y DIAGNÓSTICO DEL INCIDENTE DE INTENTO DE INTRUSIÓN O INFECCIONES

## VISUALIZAR LOS USUARIOS LOGUEADOS EN EL SISTEMA

LO PRIMERO QUE HAY QUE AVERIGUAR SON **LOS USUARIOS QUE ESTÁN UTILIZANDO EL SISTEMA, DÓNDE ESTÁN, QUÉ APLICACIONES ESTÁN USANDO Y CUÁNTO TIEMPO LLEVAN REGISTRADOS**.

SI HAY UN USUARIO CON COMPORTAMIENTOS INUSUALES COMO EL TIEMPO EXCESIVO DE UTILIZACIÓN (EN COMPARACIÓN CON SU TIEMPO HABITUAL) O LA UTILIZACIÓN DE APLICACIONES POCO FRECUENTES, PODRÁ SER INDICIO DE QUE ESE USUARIO SEA EL CAUSANTE DE LA INCIDENCIA.

# 8. GUÍA PARA LA INVESTIGACIÓN Y DIAGNÓSTICO DEL INCIDENTE DE INTENTO DE INTRUSIÓN O INFECCIONES

## VISUALIZAR LOS PROCESOS ACTIVOS

AUNQUE NO SE OBSERVE NINGÚN COMPORTAMIENTO INUSUAL EN LOS USUARIOS, ES POSIBLE QUE ALGUNO DE ELLOS HAYA DEJADO EJECUTANDO UN PROCESO.

POR ELLO, ES NECESARIO OBSERVAR **CUÁLES SON LOS PROCESOS ACTIVOS EN ESE MOMENTO** Y SI HAY ALGUNO DE ELLOS SOSPECHOSO DE SER UNA AMENAZA.

SERÁN **INDICIOS DE AMENAZA**:

- PROCESOS QUE LLEVAN ACTIVOS UN LARGO PERÍODO DE TIEMPO
- PROCESOS QUE SE INICIAN EN HORAS POCO HABITUALES
- PROCESOS QUE CONSUMEN UN NIVEL ELEVADO DE CPU
- PROCESOS QUE NO ESTÁN EJECUTADOS DESDE UN TERMINAL

# 8. GUÍA PARA LA INVESTIGACIÓN Y DIAGNÓSTICO DEL INCIDENTE DE INTENTO DE INTRUSIÓN O INFECCIONES

## INVESTIGACIÓN Y DIAGNÓSTICO DE UNA INCIDENCIA YA OCURRIDA

HAY UNA SERIE DE **RECOMENDACIONES** A TENER EN CUENTA PARA ENCONTRAR INDICIOS Y SEÑALES QUE EL INTRUSO HA PODIDO DEJAR:

- **EXAMEN DE LOS ARCHIVOS DE REGISTRO O LOGS**
- **COMPROBACIÓN DE LOS PERMISOS DEL SISTEMA**
- **CHEQUEO DE LOS ARCHIVOS BINARIOS DEL SISTEMA**
- **COMPROBACIÓN DE LOS PUERTOS ABIERTOS**
- **COMPROBAR LA EXISTENCIA DE SNIFFERS**
- **COMPROBAR LA EXISTENCIA DE SERVICIOS NO AUTORIZADOS**
- **COMPROBAR LAS CONTRASEÑAS DEL SISTEMA**
- **COMPROBAR LA CONFIGURACIÓN DEL SISTEMA Y DE LA RED**
- **BUSCAR TODOS LOS ARCHIVOS OCULTOS O POCO HABITUALES**
- **EXAMINAR TODOS LOS EQUIPOS DE LA RED LOCAL**

# 8. GUÍA PARA LA INVESTIGACIÓN Y DIAGNÓSTICO DEL INCIDENTE DE INTENTO DE INTRUSIÓN O INFECCIONES

## INVESTIGACIÓN Y DIAGNÓSTICO DE UNA INCIDENCIA YA OCURRIDA

### EXAMEN DE LOS ARCHIVOS DE REGISTRO O LOGS

CON EL EXAMEN DE LOS ARCHIVOS DE REGISTRO O LOGS **SE PODRÁ OBTENER INFORMACIÓN SOBRE CONEXIONES** A LUGARES POCO FRECUENTES, **UTILIZACIÓN DE APLICACIONES INUSUALES Y OTRAS ACTIVIDADES SOSPECHOSAS** DE INTRUSIÓN.

POR EJEMPLO, SE PUEDE OBSERVAR EL ÚLTIMO ACCESO AL SISTEMA DE UN USUARIO, LAS APLICACIONES Y PROCESOS QUE HA EJECUTADO Y LAS CONTRASEÑAS CON LAS QUE HA CONSEGUIDO ACCEDER.

SI SE DETECTA QUE ESE USUARIO NO TIENE ACCESO A ALGUNO DE LOS PROCESOS O APLICACIONES EJECUTADAS O QUE HA UTILIZADO CONTRASEÑAS QUE NO DEBERÍA CONOCER, SON CLAROS INDICIOS DE QUE ESTE ES EL CAUSANTE DE LA INCIDENCIA.

# 8. GUÍA PARA LA INVESTIGACIÓN Y DIAGNÓSTICO DEL INCIDENTE DE INTENTO DE INTRUSIÓN O INFECCIONES

## INVESTIGACIÓN Y DIAGNÓSTICO DE UNA INCIDENCIA YA OCURRIDA

### COMPROBACIÓN DE LOS PERMISOS DEL SISTEMA

ES NECESARIO **COMPROBAR LOS PERMISOS DE LOS USUARIOS** DEL SISTEMA PARA **DETECTAR SI ALGUNO DE ELLOS DISPONE DE MÁS PERMISOS DE LOS QUE DEBERÍA ESTAR AUTORIZADO**. UNA MALA ASIGNACIÓN DE PERMISOS PUEDE SER CAUSANTE DE INCIDENCIAS.

### CHEQUEO DE LOS ARCHIVOS BINARIOS DEL SISTEMA

ES HABITUAL QUE LOS INTRUSOS MODIFIQUEN LOS ARCHIVOS BINARIOS DEL SISTEMA PARA OCULTARSE E INTENTAR BORRAR HUELLAS. POR ELLO SE RECOMIENDA REALIZAR UNA **PROFUNDA REVISIÓN** DE LOS MISMOS CON EL FIN DE **COMPROBAR QUE NO HAN SUFRIDO NINGUNA ALTERACIÓN**.

# 8. GUÍA PARA LA INVESTIGACIÓN Y DIAGNÓSTICO DEL INCIDENTE DE INTENTO DE INTRUSIÓN O INFECCIONES

## INVESTIGACIÓN Y DIAGNÓSTICO DE UNA INCIDENCIA YA OCURRIDA

### COMPROBACIÓN DE LOS PUERTOS ABIERTOS

CUANDO SE HA PRODUCIDO UNA INTRUSIÓN Y EL INTRUSO YA NO ESTÁ EN EL SISTEMA ES POSIBLE QUE SE HAYA DEJADO UN PUERTO DE CONEXIÓN ABIERTO.

SE RECOMIENDA **COMPROBAR TODOS LOS PUERTOS DE CONEXIÓN ABIERTOS Y DETECTAR SI HAY ALGUNO QUE NO LO DEBERÍA ESTAR**.

EN CASO DE SER ASÍ SERÍA ACONSEJABLE COMPROBAR SI HAY ALGUNA RELACIÓN ENTRE LOS ÚLTIMOS USUARIOS DEL SISTEMA Y LA UTILIZACIÓN DE LOS PUERTOS ABIERTOS PARA DETECTAR CUÁL DE ELLOS SE HA DEJADO EL PUERTO ABIERTO.

# 8. GUÍA PARA LA INVESTIGACIÓN Y DIAGNÓSTICO DEL INCIDENTE DE INTENTO DE INTRUSIÓN O INFECCIONES

## INVESTIGACIÓN Y DIAGNÓSTICO DE UNA INCIDENCIA YA OCURRIDA

### COMPROBAR LA EXISTENCIA DE SNIFFERS

SE RECOMIENDA **VISUALIZAR LOS PROCESOS ACTIVOS PARA DETECTAR LA EJECUCIÓN DE SNIFFERS** QUE HAYAN SIDO INSTALADOS SIN AUTORIZACIÓN.

TAMBIÉN SE PUEDEN **OBSERVAR LOS ARCHIVOS DE REGISTRO Y LAS CONEXIONES AL EXTERIOR** COMO EL ENVÍO DE CORREOS ELECTRÓNICOS A CUENTAS DESCONOCIDAS Y SOSPECHOSAS.

ESTA MEDIDA ES FUNDAMENTAL, YA QUE PUEDE HABER INSTALADAS APLICACIONES DE MONITORIZACIÓN DEL TRÁFICO DE RED PARA OBSERVAR TODO EL TRÁFICO DE DATOS, INCLUYENDO DATOS COMPROMETIDOS Y CONTRASEÑAS.

# 8. GUÍA PARA LA INVESTIGACIÓN Y DIAGNÓSTICO DEL INCIDENTE DE INTENTO DE INTRUSIÓN O INFECCIONES

## INVESTIGACIÓN Y DIAGNÓSTICO DE UNA INCIDENCIA YA OCURRIDA

### COMPROBAR LA EXISTENCIA DE SERVICIOS NO AUTORIZADOS

SE ACONSEJA **COMPROBAR SI HAY DADO DE ALTA EN EL SISTEMA ALGÚN SERVICIO NO AUTORIZADO**.

TAMBIÉN ES RECOMENDABLE COMPROBAR TODAS LAS AUTORIZACIONES DE SERVICIOS QUE SE HAYAN HABILITADO Y DESHABILITADO ANTERIORMENTE PARA **DETECTAR SI HA HABIDO ALGUNA ALTERACIÓN**:

ES POSIBLE QUE ALGÚN INTRUSO HAYA HABILITADO SIN DEJAR RASTRO ALGÚN SERVICIO QUE PREVIAMENTE SE HAYA DESHABILITADO POR SEGURIDAD.

# 8. GUÍA PARA LA INVESTIGACIÓN Y DIAGNÓSTICO DEL INCIDENTE DE INTENTO DE INTRUSIÓN O INFECCIONES

## INVESTIGACIÓN Y DIAGNÓSTICO DE UNA INCIDENCIA YA OCURRIDA

### COMPROBAR LAS CONTRASEÑAS DEL SISTEMA

SE RECOMIENDA REALIZAR UNA COMPROBACIÓN DE TODAS LAS CONTRASEÑAS DEL SISTEMA PARA **DETECTAR SI HA HABIDO ALGUNA MODIFICACIÓN NO AUTORIZADA** DE LAS MISMAS.

### COMPROBAR LA CONFIGURACIÓN DEL SISTEMA Y DE LA RED

HAY QUE **EXAMINAR LOS ACCESOS EN LOS ARCHIVOS DE CONFIGURACIÓN DEL SISTEMA Y DE LA RED** PARA DETECTAR ALGÚN ACCESO NO AUTORIZADO QUE HAYA PODIDO MODIFICAR CUALQUIER PROPIEDAD O HERRAMIENTA DEL SISTEMA.

# 8. GUÍA PARA LA INVESTIGACIÓN Y DIAGNÓSTICO DEL INCIDENTE DE INTENTO DE INTRUSIÓN O INFECCIONES

## INVESTIGACIÓN Y DIAGNÓSTICO DE UNA INCIDENCIA YA OCURRIDA

### BUSCAR TODOS LOS ARCHIVOS OCULTOS O POCO HABITUALES

OTRO MODO DE COMPROBAR LA EXISTENCIA DE AMENAZAS EN EL SISTEMA ES MEDIANTE **EL CHEQUEO DE TODOS SUS ARCHIVOS**.

ES MUY FRECUENTE QUE LOS INTRUSOS SE OCULTEN EN EL SISTEMA MEDIANTE ARCHIVOS OCULTOS O INUSUALES EN LOS QUE PUEDAN OCULTAR HERRAMIENTAS Y APLICACIONES QUE LES PERMITAN SALTAR LOS SISTEMAS DE SEGURIDAD DEL SISTEMA Y ACCEDER A ARCHIVOS COMPROMETIDOS Y/O CRÍTICOS.

# 8. GUÍA PARA LA INVESTIGACIÓN Y DIAGNÓSTICO DEL INCIDENTE DE INTENTO DE INTRUSIÓN O INFECCIONES

## INVESTIGACIÓN Y DIAGNÓSTICO DE UNA INCIDENCIA YA OCURRIDA

### EXAMINAR TODOS LOS EQUIPOS DE LA RED LOCAL

NO SOLO HAY QUE EXAMINAR EL EQUIPO DEL QUE SE SOSPECHA QUE HA PODIDO SUFRIR UN ATAQUE, TAMBIÉN SE DEBEN **EXAMINAR TODOS LOS EQUIPOS QUE FORMEN PARTE DE SU RED PARA COMPROBAR SI HAN SIDO AFECTADOS**.

ES MUY HABITUAL QUE, SI UN EQUIPO HA SIDO ATACADO Y NO SE HA DETECTADO A TIEMPO, EL ATAQUE SE HAYA EXPANDIDO A VARIOS EQUIPOS DE SU RED INCREMENTANDO LOS DAÑOS CAUSADOS.

# CONTENIDOS

1. INTRODUCCIÓN
2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES
3. CATEGORIZACIÓN DE LOS INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES EN FUNCIÓN DE SU IMPACTO POTENCIAL
4. CRITERIOS PARA LA DETERMINACIÓN DE LAS EVIDENCIAS OBJETIVAS EN LAS QUE SE SOPORTARÁ LA GESTIÓN DEL INCIDENTE
5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES
6. GUÍA PARA LA CLASIFICACIÓN Y ANÁLISIS INICIAL DEL INTENTO DE INTRUSIÓN O INFECCIÓN CONTEMPLANDO EL IMPACTO PREVISIBLE DEL MISMO
7. ESTABLECIMIENTO DEL NIVEL DE INTERVENCIÓN REQUERIDO EN FUNCIÓN DEL IMPACTO PREVISIBLE
8. GUÍA PARA LA INVESTIGACIÓN Y DIAGNÓSTICO DEL INCIDENTE DE INTENTO DE INTRUSIÓN O INFECCIONES
9. **ESTABLECIMIENTO DEL PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE LOS SISTEMAS TRAS UN INCIDENTE DERIVADO DE UN INTENTO DE INTRUSIÓN O INFECCIÓN**
10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE
11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE Y LOS REGISTROS NECESARIOS PARA DOCUMENTAR EL HISTÓRICO DEL INCIDENTE

# 9. ESTABLECIMIENTO DEL PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE LOS SISTEMAS TRAS UN INCIDENTE DERIVADO DE UN INTENTO DE INTRUSIÓN O INFECCIÓN

## PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE INCIDENTES

UNA VEZ CONFIRMADO Y DIAGNOSTICADO EL INCIDENTE ES EL MOMENTO **DE PROCEDER A SU RESOLUCIÓN Y A LA RECUPERACIÓN DE LOS SISTEMAS** A LA SITUACIÓN PREVIA A SU APARICIÓN.

ESTA FASE DE RESOLUCIÓN Y RECUPERACIÓN SE DIVIDE EN TRES APARTADOS:

- **CONTENCIÓN DEL INCIDENTE**
- **MEDIDAS DE ERRADICACIÓN**
- **RECUPERACIÓN**

# 9. ESTABLECIMIENTO DEL PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE LOS SISTEMAS TRAS UN INCIDENTE DERIVADO DE UN INTENTO DE INTRUSIÓN O INFECCIÓN

## PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE INCIDENTES

### CONTENCIÓN DEL INCIDENTE

ANTES DE PROCEDER A LA ELIMINACIÓN DEL INCIDENTE, ES NECESARIO DESARROLLAR UNA **ESTRATEGIA DE CONTENCIÓN DEL INCIDENTE DE SEGURIDAD**.

CONSISTE EN **REALIZAR TODAS LAS MEDIDAS NECESARIAS PARA IMPEDIR QUE EL INCIDENTE DE SEGURIDAD SIGA PROPAGÁNDOSE Y DAÑANDO AL SISTEMA**. REALIZAR LA EJECUCIÓN DE ESTAS MEDIDAS LO MÁS RÁPID0 POSIBLE PARA MINIMIZAR LOS DAÑOS DEL SISTEMA.

*UNOS EJEMPLOS PUEDEN SER LA DESCONEXIÓN DE EQUIPOS DE LA RED O DESACTIVACIÓN DE SERVICIOS PARA EVITAR DAÑOS MAYORES.*

# 9. ESTABLECIMIENTO DEL PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE LOS SISTEMAS TRAS UN INCIDENTE DERIVADO DE UN INTENTO DE INTRUSIÓN O INFECCIÓN

## PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE INCIDENTES

### CONTENCIÓN DEL INCIDENTE

**EN CIERTAS OCASIONES**, CUANDO EL INCIDENTE NO ES CRÍTICO, **PUEDE SER MUY ÚTIL RETRASAR LA CONTENCIÓN PARA AVERIGUAR MÁS DETALLES DE LA INCIDENCIA** E IMPLANTAR NUEVAS MEDIDAS PREVENTIVAS QUE EVITEN QUE VUELVA A OCURRIR. TAMBIÉN SERVIRÍA **PARA RECOGER EVIDENCIAS DE LAS INCIDENCIAS Y DE LOS ATACANTES** QUE PERMITAN EJERCER MEDIDAS LEGALES CONTRA ELLOS.

**HAY QUE TENER MUCHO CUIDADO CON ESTA TÉCNICA** DEBIDO A LOS DAÑOS IRREPARABLES QUE PUEDE CAUSAR EL RETRASO DE LA IMPLANTACIÓN DE LAS MEDIDAS DE CONTENCIÓN.

# 9. ESTABLECIMIENTO DEL PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE LOS SISTEMAS TRAS UN INCIDENTE DERIVADO DE UN INTENTO DE INTRUSIÓN O INFECCIÓN

## PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE INCIDENTES

### MEDIDAS DE ERRADICACIÓN

CONTENIDO EL INCIDENTE, SE PUEDEN LLEVAR A CABO TODAS LAS **ACTIVIDADES Y MEDIDAS NECESARIAS PARA ELIMINAR EL INCIDENTE** EN LOS EQUIPOS Y RECURSOS AFECTADOS.

SE RECOMIENDA **ANALIZAR TODOS LOS EQUIPOS AFECTADOS PARA BUSCAR Y ELIMINAR ARCHIVOS INTRODUCIDOS POR EL INTRUSO Y CUENTAS DE USUARIO QUE CREARON PARA ACCEDER A LOS SISTEMAS**.

HAY QUE REVISAR LOS SERVICIOS Y PROCESOS AFECTADOS. REVISAR LOS DEMÁS EQUIPOS QUE FORMEN PARTE DE LA RED PARA CERCIORARSE DE LA ERRADICACIÓN COMPLETA DE LA INTRUSIÓN.

# 9. ESTABLECIMIENTO DEL PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE LOS SISTEMAS TRAS UN INCIDENTE DERIVADO DE UN INTENTO DE INTRUSIÓN O INFECCIÓN

## PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE INCIDENTES

### RECUPERACIÓN

CONFIRMADA LA ELIMINACIÓN DE LA INTRUSIÓN Y DEL INCIDENTE SE PUEDE INICIAR LA FASE DE RECUPERACIÓN.

**CONSISTIRÁ EN TAREAS DE RESTAURACIÓN DE LOS SISTEMAS** PARA QUE PUEDAN VOLVER A SU FUNCIONAMIENTO HABITUAL:

REALIZACIÓN DE TAREAS COMO LA **UTILIZACIÓN DE COPIAS DE RESPALDO** PARA REINSTALAR EL SISTEMA OPERATIVO Y LAS APLICACIONES, ADEMÁS DE LAS **ACTUALIZACIONES DE SEGURIDAD** BÁSICAS. TAMBIÉN HAY QUE VOLVER A **DEFINIR CONTRASEÑAS NUEVAS** PARA MINIMIZAR EL RIESGO DE INTRUSIONES.

# 9. ESTABLECIMIENTO DEL PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE LOS SISTEMAS TRAS UN INCIDENTE DERIVADO DE UN INTENTO DE INTRUSIÓN O INFECCIÓN

## EL PLAN DE RECUPERACIÓN ANTE DESASTRES

SE RECOMIENDA LA IMPLANTACIÓN DE **UN PLAN DE RECUPERACIÓN ANTE DESASTRES** QUE ESTABLEZCA PROCEDIMIENTOS PARA LA RECUPERACIÓN DE LA INFORMACIÓN EN CASO DE INCIDENCIAS Y DESASTRES.

EL DISEÑO SE LLEVARÁ A CABO POR UNA SERIE DE **OBJETIVOS**:

- **DETERMINACIÓN DE LAS VULNERABILIDADES**
- **IDENTIFICACIÓN Y ANÁLISIS DEL COSTE**
- **DETERMINACIÓN DE LAS NECESIDADES INMEDIATAS**
- **IDENTIFICACIÓN DE LAS DISTINTAS ALTERNATIVAS POSIBLES**
- **DESARROLLO E IMPLANTACIÓN DE PLANES DE CONTINGENCIA**

# 9. ESTABLECIMIENTO DEL PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE LOS SISTEMAS TRAS UN INCIDENTE DERIVADO DE UN INTENTO DE INTRUSIÓN O INFECCIÓN

## EL PLAN DE RECUPERACIÓN ANTE DESASTRES

### OBJETIVOS

**DETERMINACIÓN DE LAS VULNERABILIDADES** QUE PUEDAN INTERRUMPIR EL SERVICIO OFRECIDO Y DEFINICIÓN DE LAS MEDIDAS PREVENTIVAS QUE PERMITAN REDUCIR AL MÍNIMO LA PROBABILIDAD E IMPACTO DE ESTAS INTERRUPCIONES.

**IDENTIFICACIÓN Y ANÁLISIS DEL COSTE**, IMAGEN Y OTRAS CONSECUENCIAS QUE DERIVEN DE LA INTERRUPCIÓN DE LA ACTIVIDAD DE LA ORGANIZACIÓN A CAUSA DE LA INTRUSIÓN.

# 9. ESTABLECIMIENTO DEL PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE LOS SISTEMAS TRAS UN INCIDENTE DERIVADO DE UN INTENTO DE INTRUSIÓN O INFECCIÓN

## EL PLAN DE RECUPERACIÓN ANTE DESASTRES

### OBJETIVOS

**DETERMINACIÓN DE LAS NECESIDADES INMEDIATAS**, TANTO A MEDIO COMO A LARGO PLAZO, DE RECUPERACIÓN DEL SERVICIO Y DE LOS RECURSOS QUE SEAN NECESARIOS PARA ELLO.

**IDENTIFICACIÓN DE LAS DISTINTAS ALTERNATIVAS POSIBLES** Y SELECCIÓN DE LAS MÁS RENTABLES PARA FACILITAR LAS OPERACIONES DE COPIA DE SEGURIDAD Y RESTAURACIÓN DE LA ACTIVIDAD A TIEMPO.

**DESARROLLO E IMPLANTACIÓN DE PLANES DE CONTINGENCIA** QUE SE ENCARGUEN DE EJECUTAR LAS MEDIDAS INMEDIATAS Y DE LARGO PLAZO.

# 9. ESTABLECIMIENTO DEL PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE LOS SISTEMAS TRAS UN INCIDENTE DERIVADO DE UN INTENTO DE INTRUSIÓN O INFECCIÓN

## EL PLAN DE RECUPERACIÓN ANTE DESASTRES

CON EL PLAN DE RECUPERACIÓN ANTE DESASTRES DE CALIDAD **SE CONSIGUE REDUCIR AL MÍNIMO EL TIEMPO DE INACTIVIDAD DE LA ORGANIZACIÓN** POR PRODUCIRSE ALGUNA INTRUSIÓN **Y** TAMBIÉN **REDUCIR LA PÉRDIDA DE DATOS** AL MÍNIMO POSIBLE.

PARA SU ELABORACIÓN **HAY QUE REALIZAR UN ANÁLISIS DE IMPACTO** A LA ORGANIZACIÓN O AL NEGOCIO: UN INFORME EN EL QUE SE MUESTREN LOS COSTES QUE PUEDE CONLLEVAR LA APARICIÓN DE UNA INTRUSIÓN O INCIDENCIA Y LA INTERRUPCIÓN DE LA ACTIVIDAD PROVOCADA POR DICHA INTRUSIÓN.

## 9. ESTABLECIMIENTO DEL PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE LOS SISTEMAS TRAS UN INCIDENTE DERIVADO DE UN INTENTO DE INTRUSIÓN O INFECCIÓN

### EL PLAN DE RECUPERACIÓN ANTE DESASTRES

LA **ESTRUCTURA DE UN PLAN DE RECUPERACIÓN DE DESASTRES** DEBERÍA CONTENER, COMO MÍNIMO, LO SIGUIENTE:

- **PLAN DE TRABAJO** CON LA PLANIFICACIÓN DE ACTIVIDADES DE RECUPERACIÓN DE LA INFORMACIÓN.
- **INFORMES DE EVALUACIÓN DE LA SEGURIDAD** Y LA VULNERABILIDAD DE LOS SISTEMAS.
- **ANÁLISIS DE IMPACTO AL NEGOCIO**.
- **DEFINICIÓN DE LOS REQUISITOS DE LA ORGANIZACIÓN** EN CUANTO A LAS NECESIDADES DE RECUPERACIÓN, EL ÁMBITO DE APLICACIÓN Y SUS OBJETIVOS.

## 9. ESTABLECIMIENTO DEL PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE LOS SISTEMAS TRAS UN INCIDENTE DERIVADO DE UN INTENTO DE INTRUSIÓN O INFECCIÓN

### EL PLAN DE RECUPERACIÓN ANTE DESASTRES

- **PLAN DE DESARROLLO DE LA ORGANIZACIÓN** QUE ESTABLEZCA LAS NORMAS DE RECUPERACIÓN, LOS RESPONSABLES DE SEGURIDAD Y LAS COPIAS DE RESPALDO DE LA INFORMACIÓN.
- **PROGRAMA DE PRUEBAS** QUE ESTABLEZCA LAS ESTRATEGIAS DE LA ORGANIZACIÓN PARA EJECUTAR PRUEBAS, ENSAYOS Y EJERCICIOS CON EL FIN DE COMPROBAR LA SEGURIDAD DE SUS EQUIPOS Y SISTEMAS.
- **PROGRAMA DE MANTENIMIENTO** QUE ESTABLEZCA TODAS LAS MEDIDAS DE ACTUALIZACIÓN DE SISTEMAS Y DE APLICACIONES DE LOS EQUIPOS DE LA ORGANIZACIÓN.
- **PRUEBA INICIAL DEL PLAN** DE RECUPERACIÓN DE DESASTRES E IMPLANTACIÓN.

# 9. ESTABLECIMIENTO DEL PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE LOS SISTEMAS TRAS UN INCIDENTE DERIVADO DE UN INTENTO DE INTRUSIÓN O INFECCIÓN

## EL PLAN DE RECUPERACIÓN ANTE DESASTRES

HAY QUE TENER EN CUENTA QUE LAS ORGANIZACIONES ESTÁN EN CONTINUO CAMBIO Y, POR TANTO**, EL PLAN DE RECUPERACIÓN** ANTE DESASTRES NO DEBE SER ESTÁTICO, TODO LO CONTRARIO, **DEBE REVISARSE Y ACTUALIZARSE PERIÓDICAMENTE** PARA ADAPTARSE A LAS CARACTERÍSTICAS DE LOS DATOS DE LA ORGANIZACIÓN Y A LAS NECESIDADES DE SEGURIDAD Y RECUPERACIÓN DE DATOS.

# 9. ESTABLECIMIENTO DEL PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE LOS SISTEMAS TRAS UN INCIDENTE DERIVADO DE UN INTENTO DE INTRUSIÓN O INFECCIÓN

## EL PLAN DE RECUPERACIÓN ANTE DESASTRES

UN PLAN DE RESPUESTA A INCIDENTES IMPLICA NUMEROSOS **BENEFICIOS**:

- REDUCCIÓN DE DAÑOS Y PÉRDIDAS ANTE LA PRESENCIA DE UN INCIDENTE.
- MAYOR CAPACIDAD DE PROTECCIÓN DE LOS SISTEMAS CRÍTICOS PARA LA ORGANIZACIÓN.
- REDUCCIÓN DEL RIESGO DE INTERRUPCIÓN DE LA ACTIVIDAD.
- MINIMIZACIÓN DE LA TOMA DE DECISIONES EN CASO DE DETECCIÓN DE INCIDENTES.
- MEJORA DE LA EFICIENCIA GENERAL DE LA ORGANIZACIÓN CON LA IDENTIFICACIÓN DE SUS RECURSOS Y ACTIVOS CRÍTICOS.
- REDUCCIÓN DE LAS RESPONSABILIDADES LEGALES QUE PUEDAN VENIR OCASIONADAS POR LA PRODUCCIÓN DE INCIDENTES.
- GARANTÍA DE LA FIABILIDAD DE LOS SISTEMAS RESERVA DE LA ORGANIZACIÓN.

# CONTENIDOS

1. INTRODUCCIÓN
2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES
3. CATEGORIZACIÓN DE LOS INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES EN FUNCIÓN DE SU IMPACTO POTENCIAL
4. CRITERIOS PARA LA DETERMINACIÓN DE LAS EVIDENCIAS OBJETIVAS EN LAS QUE SE SOPORTARÁ LA GESTIÓN DEL INCIDENTE
5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES
6. GUÍA PARA LA CLASIFICACIÓN Y ANÁLISIS INICIAL DEL INTENTO DE INTRUSIÓN O INFECCIÓN CONTEMPLANDO EL IMPACTO PREVISIBLE DEL MISMO
7. ESTABLECIMIENTO DEL NIVEL DE INTERVENCIÓN REQUERIDO EN FUNCIÓN DEL IMPACTO PREVISIBLE
8. GUÍA PARA LA INVESTIGACIÓN Y DIAGNÓSTICO DEL INCIDENTE DE INTENTO DE INTRUSIÓN O INFECCIONES
9. ESTABLECIMIENTO DEL PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE LOS SISTEMAS TRAS UN INCIDENTE DERIVADO DE UN INTENTO DE INTRUSIÓN O INFECCIÓN
10. **PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE**
11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE Y LOS REGISTROS NECESARIOS PARA DOCUMENTAR EL HISTÓRICO DEL INCIDENTE

# 10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE

CUANDO YA SE HA LLEGADO A **CONTROLAR EL INCIDENTE** Y SE HA CONSEGUIDO **RESTAURAR LA SITUACIÓN INICIAL** ES EL MOMENTO DE **EVALUAR SI PROCEDE COMUNICAR LOS HECHOS SUCEDIDOS A TERCEROS** QUE NO TENGAN QUE VER CON LA ORGANIZACIÓN.

EN EL **PLAN DE RESPUESTA A INCIDENTES** DE LAS ORGANIZACIONES SE DEBERÍAN REFLEJAR LOS ASPECTOS REFERENTES A **LA COMUNICACIÓN A TERCEROS DE LAS INCIDENCIAS PRODUCIDAS, LOS EFECTOS CAUSADOS, SUS CAUSAS Y LAS POSIBLES CONSECUENCIAS** QUE HAYAN PODIDO SUCEDER.

LOS **PRINCIPALES AGENTES Y ACCIONES RECOMENDABLES** A LOS QUE SE LES DEBERÍA FACILITAR INFORMACIÓN SOBRE LA OCURRENCIA DE UN INCIDENTE DE SEGURIDAD SON LOS QUE SE DESCRIBEN A CONTINUACIÓN.

# 10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE

## ASESORAMIENTO

SE RECOMIENDA A LAS ORGANIZACIONES QUE INTENTEN **ASESORARSE ANTE PROFESIONALES ESPECIALIZADOS** QUE EVALÚEN LAS ACCIONES Y DECISIONES TOMADAS CON EL FIN DE MEJORAR PARA FUTURAS INCIDENCIAS.

AUNQUE SIEMPRE HAY QUE HACER UN ANÁLISIS INTERNO DE LA EVOLUCIÓN Y DE LAS DECISIONES TOMADAS ANTE LA DETECCIÓN DE UN INCIDENTE, SIEMPRE **ES ACONSEJABLE LA OPINIÓN DE UN ENTE PROFESIONAL EXTERNO.**

# 10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE

## PROVEEDORES

SI LOS SISTEMAS IDS/IPS HAN FALLADO, HAY QUE **RECURRIR A LOS PROVEEDORES DE** DICHAS **HERRAMIENTAS** PARA QUE SEAN CONSCIENTES DE LOS FALLOS DE SU APLICACIÓN.

**CUALQUIER INCIDENCIA DESCONOCIDA POR EL PROVEEDOR**, EN EL CASO DE DETECTARSE EN LA ORGANIZACIÓN, **DEBERÍA SER REPORTADA PARA REALICEN ACTUALIZACIONES** QUE IMPIDAN LA SUCESIÓN DE ESTAS INCIDENCIAS EN EL FUTURO.

TAMBIÉN ES RECOMENDABLE **VALORAR LAS ALTERNATIVAS DE OTROS PROVEEDORES** ANALIZANDO EL COSTE QUE SUPONDRÍA LA IMPLANTACIÓN DE NUEVAS HERRAMIENTAS Y LAS VENTAJAS QUE ESA IMPLANTACIÓN PUEDE SUPONER.

# 10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE

## COMUNICACIÓN A TERCEROS

APARTE DE LOS PROVEEDORES **ES POSIBLE QUE LA INCIDENCIA HAYA AFECTADO A DATOS Y RECURSOS DE TERCERAS** PERSONAS Y/O ORGANIZACIONES.

ES CONVENIENTE **COMUNICAR** A ESTOS **TERCEROS LA DETECCIÓN DE LA INCIDENCIA, LAS PRINCIPALES ACTUACIONES REALIZADAS Y LAS CONSECUENCIAS DE LA MISMA** PARA QUE SEAN CONSCIENTES DEL FALLO Y PUEDAN COLABORAR EN LA RESTAURACIÓN DE LA SITUACIÓN ORIGINAL.

# 10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE

## FABRICANTES DE SOFTWARE Y HARDWARE

EN EL MOMENTO EN EL QUE LA INCIDENCIA HA AFECTADO A ALGÚN COMPONENTE DE SOFTWARE O HARDWARE DE LA ORGANIZACIÓN SE RECOMIENDA **COMUNICARLO A SUS PROVEEDORES Y FABRICANTES** PARA QUE EVALÚEN LOS DAÑOS CAUSADOS Y LAS POSIBLES CONSECUENCIAS QUE PUEDAN APARECER.

TAMBIÉN SE ACONSEJA CONTACTAR CON ELLOS PARA COMPROBAR SI NO HA SIDO ALGUNA VULNERABILIDAD DE SUS APLICACIONES O DISPOSITIVOS LOS QUE HAYAN PERMITIDO EL ACCESO DEL INTRUSO AL SISTEMA.

# 10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE

## COMUNICACIÓN A TERCEROS PERJUDICADOS

NO SOLO HAY QUE COMUNICAR A LOS TERCEROS CUYOS RECURSOS HAN SIDO AFECTADOS A NIVEL INTERNO DE LA ORGANIZACIÓN.

HAY QUE EVALUAR LOS DAÑOS PROVOCADOS POR EL INCIDENTE Y LOS DATOS MODIFICADOS O PERDIDOS PARA **COMPROBAR SI SE HA PUESTO EN PELIGRO LA SEGURIDAD, PRIVACIDAD E INTEGRIDAD DE DATOS DE TERCEROS.**

# 10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE

## COMUNIDAD GENERAL

CUANDO LA GRAVEDAD DE LA INCIDENCIA SUPONE CONSECUENCIAS GRAVES PARA LA ORGANIZACIÓN E INCLUSO DAÑOS Y CONSECUENCIAS PERJUDICIALES PARA LA COMUNIDAD, ES RECOMENDABLE COMUNICAR LA APARICIÓN DE DICHA INCIDENCIA Y DE LAS CONSECUENCIAS DE SU INFECCIÓN EN LOS SISTEMAS Y APLICACIONES DE UNA ORGANIZACIÓN Y/O USUARIO PARTICULAR A TRAVÉS DE UN **PLAN DE COMUNICACIÓN CON LOS MEDIOS.**

# 10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE

## FUERZAS DE SEGURIDAD

EN EL CASO DE HABERSE PRODUCIDO **DELITO INFORMÁTICO** POR PARTE DEL ATACANTE HAY **QUE COMUNICAR** TODO LO SUCEDIDO **A LA POLICÍA O AGENTE DE SEGURIDAD ANÁLOGO** PARA QUE RECABEN TODO TIPO DE PRUEBAS Y HUELLAS Y CONSEGUIR LOCALIZARLE PARA QUE CUMPLA CON LOS REQUERIMIENTOS LEGALES.

# 10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE

## ORGANISMOS DE RESPUESTA A INCIDENTES

LAS ORGANIZACIONES DEBEN **ESTAR EN CONTACTO CON LOS ORGANISMOS DE RESPUESTA A INCIDENTES** COMO **INCIBE-CERT, CCN-CERT** EN ESPAÑA U OTROS ORGANISMOS INTERNACIONALES.

ESTOS ORGANISMOS FACILITARÁN UN APOYO CONSTANTE Y AYUDA EN EL MOMENTO DE COMBATIR INCIDENCIAS QUE PUEDAN SURGIR EN LA ORGANIZACIÓN.

TAMBIÉN ES RECOMENDABLE COMUNICAR LA INCIDENCIA PARA QUE SEA EVALUADA POR UN EQUIPO DE EXPERTOS Y, EN CASO DE SER NECESARIO, INCORPORARLA A SU BASE DE DATOS PARA PONER EN CONOCIMIENTO PÚBLICO SU POSIBLE APARICIÓN Y CÓMO DETECTARLA Y COMBATIRLA.

# CONTENIDOS

1. INTRODUCCIÓN
2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES
3. CATEGORIZACIÓN DE LOS INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES EN FUNCIÓN DE SU IMPACTO POTENCIAL
4. CRITERIOS PARA LA DETERMINACIÓN DE LAS EVIDENCIAS OBJETIVAS EN LAS QUE SE SOPORTARÁ LA GESTIÓN DEL INCIDENTE
5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES
6. GUÍA PARA LA CLASIFICACIÓN Y ANÁLISIS INICIAL DEL INTENTO DE INTRUSIÓN O INFECCIÓN CONTEMPLANDO EL IMPACTO PREVISIBLE DEL MISMO
7. ESTABLECIMIENTO DEL NIVEL DE INTERVENCIÓN REQUERIDO EN FUNCIÓN DEL IMPACTO PREVISIBLE
8. GUÍA PARA LA INVESTIGACIÓN Y DIAGNÓSTICO DEL INCIDENTE DE INTENTO DE INTRUSIÓN O INFECCIONES
9. ESTABLECIMIENTO DEL PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE LOS SISTEMAS TRAS UN INCIDENTE DERIVADO DE UN INTENTO DE INTRUSIÓN O INFECCIÓN
10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE
11. **ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE Y LOS REGISTROS NECESARIOS PARA DOCUMENTAR EL HISTÓRICO DEL INCIDENTE**

# 11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE Y LOS REGISTROS NECESARIOS PARA DOCUMENTAR EL HISTÓRICO DEL INCIDENTE

**DURANTE TODO EL CICLO DE VIDA DEL INCIDENTE HAY QUE ELABORAR Y MANTENER UN REGISTRO** SOBRE TODAS LAS ACCIONES QUE SE VAN TOMANDO Y SU EVOLUCIÓN PARA QUE LOS AGENTES ENCARGADOS DE LA SOLUCIÓN Y LOS USUARIOS AFECTADOS DISPONGAN DE INFORMACIÓN ACTUALIZADA SOBRE EL ESTADO DEL INCIDENTE.

# 11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE Y LOS REGISTROS NECESARIOS PARA DOCUMENTAR EL HISTÓRICO DEL INCIDENTE

CUANDO YA SE HA SOLUCIONADO HAY QUE LLEVAR A CABO UNA SERIE DE **ACCIONES QUE PERMITAN CERRAR EL INCIDENTE**:

- COMPROBAR CON LOS USUARIOS QUE EL INCIDENTE HA SIDO SOLUCIONADO SATISFACTORIAMENTE.
- INCORPORAR LAS ACCIONES Y MEDIDAS TOMADAS PARA LA RESOLUCIÓN DEL INCIDENTE EN LA BASE DE DATOS DE SU HISTÓRICO.
- RECLASIFICAR EL INCIDENTE COMO “RESUELTO” O “CERRADO”.
- ACTUALIZAR LA INFORMACIÓN (EN LA BASE DE DATOS DE LA ORGANIZACIÓN) DE LAS CONFIGURACIONES DEL SISTEMA QUE HAN INTERVENIDO EN EL PROCESO DE GESTIÓN DEL INCIDENTE.
- CERRAR EL INCIDENTE.

# 11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE Y LOS REGISTROS NECESARIOS PARA DOCUMENTAR EL HISTÓRICO DEL INCIDENTE

A PESAR DE ESTAR RESUELTO Y SOLUCIONADO EL PROCESO DE GESTIÓN DEL INCIDENTE NO TERMINA AHÍ, SINO QUE **SERÁ NECESARIO LA ELABORACIÓN DE INFORMES** QUE SIRVAN PARA COMPARAR FUTURAS INCIDENCIAS Y COMPROBAR LA EFICACIA DE LAS MEDIDAS TOMADAS.

ESTOS INFORMES **DEBERÁN APORTAR INFORMACIÓN BÁSICA** COMO LOS ELEMENTOS QUE SE MENCIONAN A CONTINUACIÓN:

- **GESTIÓN DE LOS NIVELES DE SERVICIO**
- **MONITORIZACIÓN DEL RENDIMIENTO DEL CENTRO DE SERVICIOS**
- **OPTIMIZACIÓN DE LA ASIGNACIÓN DE RECURSOS**
- **IDENTIFICACIÓN DE LOS ERRORES**
- **DISPOSICIÓN DE INFORMACIÓN ESTADÍSTICA**

# 11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE Y LOS REGISTROS NECESARIOS PARA DOCUMENTAR EL HISTÓRICO DEL INCIDENTE

## GESTIÓN DE LOS NIVELES DE SERVICIO

**LOS CLIENTES DEBEN ESTAR INFORMADOS** CONVENIENTEMENTE **SOBRE LOS SERVICIOS OFRECIDOS** POR LA ORGANIZACIÓN **Y SU NIVEL DE CUMPLIMIENTO**. EN CASO DE HABER ALGÚN INCUMPLIMIENTO EN EL OFRECIMIENTO DEL SERVICIO DEBERÁN TOMARSE LAS MEDIDAS OPORTUNAS PARA SU CORRECCIÓN.

## MONITORIZACIÓN DEL RENDIMIENTO DEL CENTRO DE SERVICIOS

HAY QUE **REALIZAR ENCUESTAS Y ENTREVISTAS A LOS CLIENTES** PARA CONOCER SU NIVEL DE SATISFACCIÓN POR EL SERVICIO PRESTADO Y PARA CONTROLAR QUE LA ATENCIÓN AL CLIENTE ESTÁ DISPONIBLE EN TODO MOMENTO.

# 11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE Y LOS REGISTROS NECESARIOS PARA DOCUMENTAR EL HISTÓRICO DEL INCIDENTE

## OPTIMIZACIÓN DE LA ASIGNACIÓN DE RECURSOS

DEBE REALIZARSE UNA **EVALUACIÓN DEL PROCESO DE GESTIÓN DEL INCIDENTE** PARA COMPROBAR QUE NO HA HABIDO DUPLICIDADES Y CONSUMO DE RECURSOS INNECESARIOS.

## IDENTIFICACIÓN DE LOS ERRORES

CABE LA POSIBILIDAD QUE EL PROCEDIMIENTO SEGUIDO PARA GESTIONAR LA INCIDENCIA NO SEA FIEL A LAS DIRECTRICES DE LA ORGANIZACIÓN, A SU ESTRUCTURA O A LAS NECESIDADES. EN CASO DE SER ASÍ HABRÁ QUE **ADOPTAR MEDIDAS CORRECTIVAS PARA QUE EN FUTURAS INCIDENCIAS NO VUELVA A OCURRIR**.

# 11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE Y LOS REGISTROS NECESARIOS PARA DOCUMENTAR EL HISTÓRICO DEL INCIDENTE

## DISPOSICIÓN DE INFORMACIÓN ESTADÍSTICA

EN EL INFORME SE RECOMIENDA **INCLUIR INFORMACIÓN ESTADÍSTICA SOBRE CIERTOS PARÁMETROS SIGNIFICATIVOS** DE LA ORGANIZACIÓN (COMO CONSUMO DE RECURSOS, COSTES DEL SERVICIO, TIEMPO DE RESPUESTA, ETC.) PARA HACER PREVISIONES DE FUTURAS ACTUACIONES ANTE APARICIONES DE INCIDENTES DE SEGURIDAD.

# 11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE Y LOS REGISTROS NECESARIOS PARA DOCUMENTAR EL HISTÓRICO DEL INCIDENTE

ADEMÁS DEL INFORME **SE RECOMIENDA LA UTILIZACIÓN DE MÉTRICAS E INDICADORES** QUE SIRVAN DE COMPARACIÓN CON FUTURAS ACTUACIONES PARA UN CORRECTO SEGUIMIENTO DEL INCIDENTE. LOS PRINCIPALES ASPECTOS A CONSIDERAR SON LOS SIGUIENTES:

- CANTIDAD DE INCIDENTES CLASIFICADOS TEMPORALMENTE Y POR PRIORIDADES.
- RATIO EN PORCENTAJE DE LOS INCIDENTES (CLASIFICADOS POR PRIORIDADES) RESUELTOS EN UNA PRIMERA INSTANCIA.
- NIVEL DE CUMPLIMIENTO DE LA OFERTA DE SERVICIOS A CLIENTES.
- COSTES ASOCIADOS A LA APARICIÓN Y RESOLUCIÓN DE LA INCIDENCIA.
- RECURSOS UTILIZADOS PARA LA RESOLUCIÓN DE LA INCIDENCIA.
- NIVEL DE SATISFACCIÓN DE LOS CLIENTES.
- TIEMPOS DE RESPUESTA Y RESOLUCIÓN SEGÚN EL IMPACTO Y LA URGENCIA DE LOS INCIDENTES.

# 11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE Y LOS REGISTROS NECESARIOS PARA DOCUMENTAR EL HISTÓRICO DEL INCIDENTE

## SOPORTE DE INCIDENTES

EN CONCLUSIÓN, DESDE QUE SE DETECTA UN INCIDENTE HASTA QUE SE CIERRA **HAY UNA SERIE DE ACCIONES DE SOPORTE QUE DEBEN LLEVARSE A CABO PARA TENER UN CONTROL ADECUADO DE SU EVOLUCIÓN** Y DE TODAS LAS ACCIONES REALIZADAS PARA SU RESOLUCIÓN Y CIERRE. LOS **PASOS** A TOMAR SE DESCRIBEN A CONTINUACIÓN.

- **REPORTE DEL INCIDENTE**
- **REGISTRO Y DOCUMENTACIÓN DEL INCIDENTE**
- **PREPARACIÓN DE LA SOLUCIÓN DEL INCIDENTE**
- **APLICACIÓN DE SOLUCIONES CON SOFTWARE DE APOYO**
- **IDENTIFICACIÓN Y SOLUCIÓN DE PROBLEMAS**
- **CIERRE DEL INCIDENTE CON ÉXITO**

# 11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE Y LOS REGISTROS NECESARIOS PARA DOCUMENTAR EL HISTÓRICO DEL INCIDENTE

## SOPORTE DE INCIDENTES

### REPORTE DEL INCIDENTE

NADA MÁS DETECTAR LA **POSIBILIDAD DE SUFRIR ALGÚN ATAQUE O INCIDENCIA** (AUNQUE POSTERIORMENTE SEA UNA FALSA ALARMA**) ES NECESARIO REALIZAR SU REPORTE** PARA QUE ESTA SE ATENDIDA.

DE ESTE MODO, CUALQUIER FUNCIONAMIENTO ANORMAL O ACTIVIDAD INUSUAL DEBERÁ REPORTARSE A LOS RESPONSABLES DE LA GESTIÓN DE INCIDENTES MEDIANTE CORREO ELECTRÓNICO, TELÉFONO, PERSONALMENTE O CUALQUIER OTRO MEDIO DE COMUNICACIÓN ESTABLECIDO QUE ASEGURE SU RECEPCIÓN.

# 11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE Y LOS REGISTROS NECESARIOS PARA DOCUMENTAR EL HISTÓRICO DEL INCIDENTE

## SOPORTE DE INCIDENTES

### REGISTRO Y DOCUMENTACIÓN DEL INCIDENTE

EL RESPONSABLE DE LA GESTIÓN DEL INCIDENTE SE ENCARGARÁ DE **IDENTIFICAR EL TIPO DE INCIDENTE REMITIDO POR LOS USUARIOS Y SI ESTE ES UN INCIDENTE REAL O**, POR EL CONTRARIO, ES **UNA FALSA ALARMA**.

CON LA RECOLECCIÓN DE INFORMACIÓN QUE CONFIRME LA INCIDENCIA REAL SE PROCEDERÁ A REGISTRAR TODOS SUS DATOS Y A SU CLASIFICACIÓN SEGÚN SU PRIORIDAD, TENIENDO EN CUENTA SU IMPACTO Y LA CRITICIDAD DE LOS RECURSOS AFECTADOS.

# 11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE Y LOS REGISTROS NECESARIOS PARA DOCUMENTAR EL HISTÓRICO DEL INCIDENTE

## SOPORTE DE INCIDENTES

### PREPARACIÓN DE LA SOLUCIÓN DEL INCIDENTE

UNA VEZ REGISTRADA LA INFORMACIÓN BÁSICA DEL **INCIDENTE DEBE ASIGNARSE UN TIEMPO MÁXIMO DE RESPUESTA, CONTENCIÓN Y RESOLUCIÓN ATENDIENDO A LA PRIORIDAD** DESIGNADA A DICHO INCIDENTE.

DEBE REALIZARSE UN PROCESO DE **CONSULTA** EN LA BASE DE DATOS DE **INCIDENTES ANTIGUOS** PARA COMPROBAR SI HAY ALGÚN CASO SIMILAR Y CÓMO SE HA SOLUCIONADO ANTERIORMENTE PARA INTENTAR APLICAR MEDIDAS PARECIDAS ANTE EL INCIDENTE ACTUAL.

# 11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE Y LOS REGISTROS NECESARIOS PARA DOCUMENTAR EL HISTÓRICO DEL INCIDENTE

## SOPORTE DE INCIDENTES

### APLICACIÓN DE SOLUCIONES CON SOFTWARE DE APOYO

DENTRO DEL TIEMPO MÁXIMO DE RESOLUCIÓN DEL INCIDENTE SE PROCEDERÁ A **ENVIAR ALERTAS Y NOTIFICACIONES A LOS USUARIOS RESPONSABLES DE DICHA RESOLUCIÓN** EN CASO DE SER NECESARIO.

TAMBIÉN SE LLEVARÁN A CABO **TAREAS DE CARÁCTER INTERNO** PARA COMPLETAR Y APOYAR LAS ACTIVIDADES Y MEDIDAS QUE SE TOMARÁN PARA LA RESOLUCIÓN DEL INCIDENTE.

ASIMISMO**, SE IRÁ COMUNICANDO PERIÓDICAMENTE** DE LOS AVANCES EN SU RESOLUCIÓN **A LOS USUARIOS IMPLICADOS** EN LA INCIDENCIA.

# 11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE Y LOS REGISTROS NECESARIOS PARA DOCUMENTAR EL HISTÓRICO DEL INCIDENTE

## SOPORTE DE INCIDENTES

### IDENTIFICACIÓN Y SOLUCIÓN DE PROBLEMAS

EN EL PROCESO DE RESOLUCIÓN DE LA INCIDENCIA **SE COMPROBARÁ EL HISTÓRICO DE INCIDENCIAS.**

SI SE COMPRUEBA LA SUCESIÓN DE INCIDENCIAS RECURRENTES HABRÁ QUE DETECTAR SI HAY ALGUNA CAUSA COMÚN QUE LAS PUEDA PROVOCAR PARA EVITAR INCIDENCIAS FUTURAS Y MEJORAR LA SEGURIDAD DE LA ORGANIZACIÓN.

# 11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE Y LOS REGISTROS NECESARIOS PARA DOCUMENTAR EL HISTÓRICO DEL INCIDENTE

## SOPORTE DE INCIDENTES

### CIERRE DEL INCIDENTE CON ÉXITO

DEBE **COMUNICARSE EL CIERRE DEL INCIDENTE A LOS USUARIOS QUE HAN VISTO AFECTADO SUS DATOS** INDICANDO QUE SE HAN CUMPLIDO LOS PLAZOS PREVISTOS Y LAS POLÍTICAS DE GESTIÓN UTILIZADAS PARA LA RESOLUCIÓN DEL INCIDENTE.

TAMBIÉN SE INCLUIRÁ EL CIERRE Y LAS SOLUCIONES APLICADAS A LA BASE DE DATOS DE INCIDENTES COMO SOLUCIONES SUGERIDAS EN FUTURAS INCIDENCIAS.

# 11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE Y LOS REGISTROS NECESARIOS PARA DOCUMENTAR EL HISTÓRICO DEL INCIDENTE

## SOPORTE DE INCIDENTES

| Pasos de soporte de incidentes | Descripción |
|---|---|
| Reporte del incidente | Comunicación de las sospechas de incidente a los responsables. |
| Registro y documentación | Obtención de información adicional y clasificación de la incidencia. |
| Preparación de la solución | Asignación de tiempos máximos de contención y respuesta. |
| Aplicación de soluciones mediante software de apoyo | Remisión a los interesados de información referente a la evolución del incidente. |
| Identificación y solución de problemas | Búsqueda de causa común con incidentes anteriores. |
| Cierre del incidente con éxito | Comunicación del cierre exitoso del incidente a todos los interesados. |

# CONTENIDOS

1. INTRODUCCIÓN
2. ESTABLECIMIENTO DE LAS RESPONSABILIDADES EN EL PROCESO DE NOTIFICACIÓN Y GESTIÓN DE INTENTOS DE INTRUSIÓN O INFECCIONES
3. CATEGORIZACIÓN DE LOS INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES EN FUNCIÓN DE SU IMPACTO POTENCIAL
4. CRITERIOS PARA LA DETERMINACIÓN DE LAS EVIDENCIAS OBJETIVAS EN LAS QUE SE SOPORTARÁ LA GESTIÓN DEL INCIDENTE
5. ESTABLECIMIENTO DEL PROCESO DE DETECCIÓN Y REGISTRO DE INCIDENTES DERIVADOS DE INTENTOS DE INTRUSIÓN O INFECCIONES
6. GUÍA PARA LA CLASIFICACIÓN Y ANÁLISIS INICIAL DEL INTENTO DE INTRUSIÓN O INFECCIÓN CONTEMPLANDO EL IMPACTO PREVISIBLE DEL MISMO
7. ESTABLECIMIENTO DEL NIVEL DE INTERVENCIÓN REQUERIDO EN FUNCIÓN DEL IMPACTO PREVISIBLE
8. GUÍA PARA LA INVESTIGACIÓN Y DIAGNÓSTICO DEL INCIDENTE DE INTENTO DE INTRUSIÓN O INFECCIONES
9. ESTABLECIMIENTO DEL PROCESO DE RESOLUCIÓN Y RECUPERACIÓN DE LOS SISTEMAS TRAS UN INCIDENTE DERIVADO DE UN INTENTO DE INTRUSIÓN O INFECCIÓN
10. PROCESO PARA LA COMUNICACIÓN DEL INCIDENTE A TERCEROS, SI PROCEDE
11. ESTABLECIMIENTO DEL PROCESO DE CIERRE DEL INCIDENTE Y LOS REGISTROS NECESARIOS PARA DOCUMENTAR EL HISTÓRICO DEL INCIDENTE

# RESUMEN

**LAS INTRUSIONES** SON UN CONJUNTO DE EVENTOS OCURRIDOS CUANDO UN USUARIO INTENTA ACCEDER AL SISTEMA SIN AUTORIZACIÓN POR VARIOS MOTIVOS.

LAS ORGANIZACIONES DEBEN SER CAPACES DE **ESTABLECER UNA SERIE DE HERRAMIENTAS Y CONTROLES** QUE PREVENGAN LA APARICIÓN DE ESTOS INTRUSOS Y EVITEN SU ACCESO.

AUN ASÍ, **CUANDO SE DETECTA UNA POSIBLE INTRUSIÓN** ES NECESARIO LLEVAR A CABO UNA SERIE DE PASOS ESTABLECIDOS PARA QUE SE GESTIONE DEL MODO MÁS EFICIENTE POSIBLE.

# RESUMEN

SE COMIENZA CON LA **RECOLECCIÓN DE INFORMACIÓN ADICIONAL** PARA COMPROBAR SI LA AMENAZA ES REAL O POR EL CONTRARIO ES UNA FALSA ALARMA.

EN EL CASO DE SER UNA AMENAZA REAL SE DEBE PROCEDER A **UN ANÁLISIS DE LA INCIDENCIA Y A SU CLASIFICACIÓN** SEGÚN CRITERIOS DE CRITICIDAD DE LOS RECURSOS E IMPACTO POTENCIAL EN LA ORGANIZACIÓN.

ATENDIENDO A ESTA CLASIFICACIÓN SE DEBERÁN **DEFINIR LOS TIEMPOS MÁXIMOS DE CONTENCIÓN Y RESOLUCIÓN DEL INCIDENTE**, DEBIENDO RESOLVERSE EN MENOR TIEMPO A MEDIDA QUE AUMENTA LA PRIORIDAD DE LA INCIDENCIA.

# RESUMEN

UNA VEZ TOMADAS LAS MEDIDAS CORRECTIVAS Y RESUELTA LA INCIDENCIA DEBE VALORARSE LA POSIBILIDAD DE **COMUNICAR SU OCURRENCIA A TERCEROS** QUE PUEDAN VERSE IMPLICADOS POR LA UTILIZACIÓN DE SUS DATOS.

PARA CONCLUIR Y UNA VEZ RESUELTO EL PROBLEMA Y REALIZADAS LAS COMUNICACIONES PERTINENTES SE PROCEDERÁ AL **CIERRE DEL INCIDENTE**, REGISTRANDO TODA LA INFORMACIÓN SOBRE SU EVOLUCIÓN, LAS MEDIDAS QUE SE HAN TOMADO, LOS ERRORES COMETIDOS Y SUS SOLUCIONES PARA AUMENTAR LA EFICIENCIA ANTE INCIDENCIAS FUTURAS.

# RESUMEN

UN CORRECTO REGISTRO DEL INCIDENTE PERMITIRÁ A LAS ORGANIZACIONES **OBTENER UN APRENDIZAJE DE LAS ACCIONES TOMADAS QUE CONSIGA EVITAR NUEVOS INCIDENTES** QUE SEAN SIMILARES A LOS YA SUCEDIDOS, REDUCIÉNDOSE ASÍ TIEMPO Y DAÑOS PRODUCIDOS.

# ESTO ES TODO