IFCT0109. SEGURIDAD INFORMÁTICA

MF0488_3 GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

UD04

UNIDAD 04. RESPUESTA ANTE INCIDENTES DE SEGURIDAD

DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

CONTENIDOS

1. INTRODUCCIÓN
2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD
3. EXPOSICIÓN DE LAS DISTINTAS TÉCNICAS Y HERRAMIENTAS UTILIZADAS PARA EL ANÁLISIS Y CORRELACIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD
4. PROCESO DE VERIFICACIÓN DE LA INTRUSIÓN
5. NATURALEZA Y FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES TIPO CERT NACIONALES E INTERNACIONALES

1. INTRODUCCIÓN

CUANDO, A PESAR DE TODAS LAS MEDIDAS DE PREVENCIÓN Y CONTENCIÓN IMPLANTADAS, **SE PRODUCE UN INCIDENTE** Y CONSIGUE LLEGAR A LOS EQUIPOS DE UNA ORGANIZACIÓN RESULTA PRIMORDIAL **ESTABLECER UN PLAN DE RESPUESTA** QUE PERMITA SU ELIMINACIÓN Y LA REDUCCIÓN DE LOS DAÑOS PROVOCADOS AL MÍNIMO POSIBLE.

1. INTRODUCCIÓN

VEREMOS LAS **RECOMENDACIONES Y FASES A SEGUIR** CUANDO SE PRODUCE UN INCIDENTE DE ESTE TIPO.

EN PRIMER LUGAR, **LA RECOLECCIÓN DE TODA LA INFORMACIÓN** POSIBLE **DEL INCIDENTE** PARA IDENTIFICARLO Y PODER RESTAURAR LOS EQUIPOS A SU SITUACIÓN DE ORIGEN.

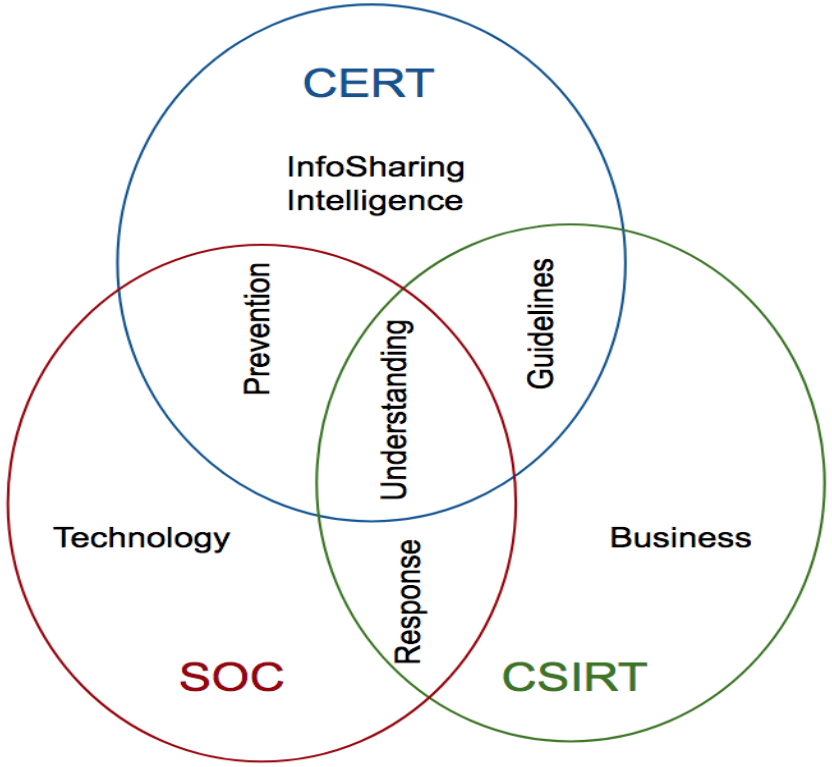
1. INTRODUCCIÓN

EN OTRA FASE SE UTILIZAN **TÉCNICAS Y HERRAMIENTAS QUE ANALICEN LA INFORMACIÓN DE LOS EVENTOS DE SEGURIDAD** PARA CONOCER CON PRECISIÓN QUÉ HA SUCEDIDO DURANTE EL INCIDENTE DE SEGURIDAD Y OBTENER PISTAS DE CÓMO SE HA PODIDO PRODUCIR.

ES POSIBLE QUE SIMPLEMENTE **SEA UNA FALSA INTRUSIÓN** Y SE ESTÉN GENERANDO ALARMAS INNECESARIAMENTE, POR LO QUE HAY QUE **VERIFICAR LA INTRUSIÓN.**

1. INTRODUCCIÓN

AL FINAL, SE MUESTRAN UNA SERIE DE **ORGANIZACIONES NACIONALES E INTERNACIONALES QUE OFRECEN APOYO E INFORMACIÓN A LAS ORGANIZACIONES Y USUARIOS ANTE LA GESTIÓN DE INCIDENTES** PARA COMPLEMENTAR Y AYUDAR A LA ELABORACIÓN DE LOS PLANES DE RESPUESTA A INCIDENTES Y ASÍ CONSEGUIR COMBATIRLOS DE UN MODO MÁS EFICAZ MINIMIZANDO LOS RIESGOS DE SEGURIDAD.



CONTENIDOS

1. INTRODUCCIÓN
2. **PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD**
3. EXPOSICIÓN DE LAS DISTINTAS TÉCNICAS Y HERRAMIENTAS UTILIZADAS PARA EL ANÁLISIS Y CORRELACIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD
4. PROCESO DE VERIFICACIÓN DE LA INTRUSIÓN
5. NATURALEZA Y FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES TIPO CERT NACIONALES E INTERNACIONALES

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

UN INCIDENTE DE SEGURIDAD ES ***UN EVENTO O CONJUNTO DE EVENTOS QUE PUEDEN PROVOCAR LA INTERRUPCIÓN DE LOS SERVICIOS OFRECIDOS POR UN SISTEMA INFORMÁTICO E INCLUSO LA PÉRDIDA DE INFORMACIÓN Y DE ACTIVOS VALIOSOS PARA LA ORGANIZACIÓN.***

LA **SEGURIDAD DE LA INFORMACIÓN** CONSISTE EN EL **ESTABLECIMIENTO DE UNA SERIE DE MEDIDAS** POR PARTE DE LAS ORGANIZACIONES QUE PERMITAN PROTEGER LA INFORMACIÓN MANTENIENDO SUS PROPIEDADES DE *CONFIDENCIALIDAD, DISPONIBILIDAD E INTEGRIDAD*.

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

ESTAS MEDIDAS SE CLASIFICAN EN:

- **MEDIDAS PREVENTIVAS**
- **MEDIDAS CORRECTIVAS**
- **MEDIDAS DE DETECCIÓN**

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

MEDIDAS PREVENTIVAS

ESTABLECIMIENTO DE CONTRASEÑAS, POLÍTICAS DE SEGURIDAD, CORTAFUEGOS, PROCEDIMIENTOS DE COPIAS DE RESPALDO, CONCIENCIACIÓN DEL PERSONAL, ETC.

MEDIDAS CORRECTIVAS

PROCEDIMIENTOS DE RESTAURACIÓN DEL SISTEMA, ESTABLECIMIENTO DE ESQUEMAS DE TOLERANCIA A FALLOS, ETC.

MEDIDAS DE DETECCIÓN

REVISIONES DE SEGURIDAD, ANÁLISIS DE REGISTROS DE AUDITORÍA, ANÁLISIS DE LOGS, ETC.

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

LA **GESTIÓN DE INCIDENTES DE SEGURIDAD** ES ***LA PARTE DE LA SEGURIDAD DE LA INFORMACIÓN ENCARGADA DE ASIGNAR LOS RECURSOS ADECUADOS Y NECESARIOS A LA PREVENCIÓN, DETECCIÓN Y CORRECCIÓN DE INCIDENTES QUE AFECTEN A LA SEGURIDAD DE LA INFORMACIÓN…***

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

LOS **BENEFICIOS** DE APLICAR UNA GESTIÓN DE INCIDENTES SON:

- RESPUESTA SISTEMÁTICA A LOS INCIDENTES DE SEGURIDAD.
- AGILIZA Y FACILITA EL PROCESO DE RECUPERACIÓN DE EQUIPOS Y SISTEMAS ANTE EL ACONTECIMIENTO DE INCIDENTES DE SEGURIDAD.
- REDUCE LA PÉRDIDA DE DATOS Y EL TIEMPO DE INTERRUPCIÓN DE SERVICIOS.
- A TRAVÉS DEL APRENDIZAJE SE PREVIENEN LOS INCIDENTES REITERADOS.
- MEJORA CONTINUA DE LA SEGURIDAD DE LA ORGANIZACIÓN Y DEL PROCESO DE GESTIÓN Y TRATAMIENTO DE INCIDENTES.
- FACILITA LA GESTIÓN DE LOS ASPECTOS LEGALES REFERENTES A LOS INCIDENTES DE SEGURIDAD.

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

EQUIPO DE RESPUESTA DE INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT)

EL TÉRMINO **CSIRT** (**COMPUTER SECURITY INCIDENT RESPONSE TEAM**) SURGIÓ ANTE LA NECESIDAD DE DESIGNAR ***UN CONJUNTO DE PERSONAS ESPECIALIZADAS ENCARGADAS ESPECÍFICAMENTE DE LA GESTIÓN Y TRATAMIENTO DE INCIDENTES.***

CSIRT

Equipo de Respuesta ante Incidentes de Seguridad Informática

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

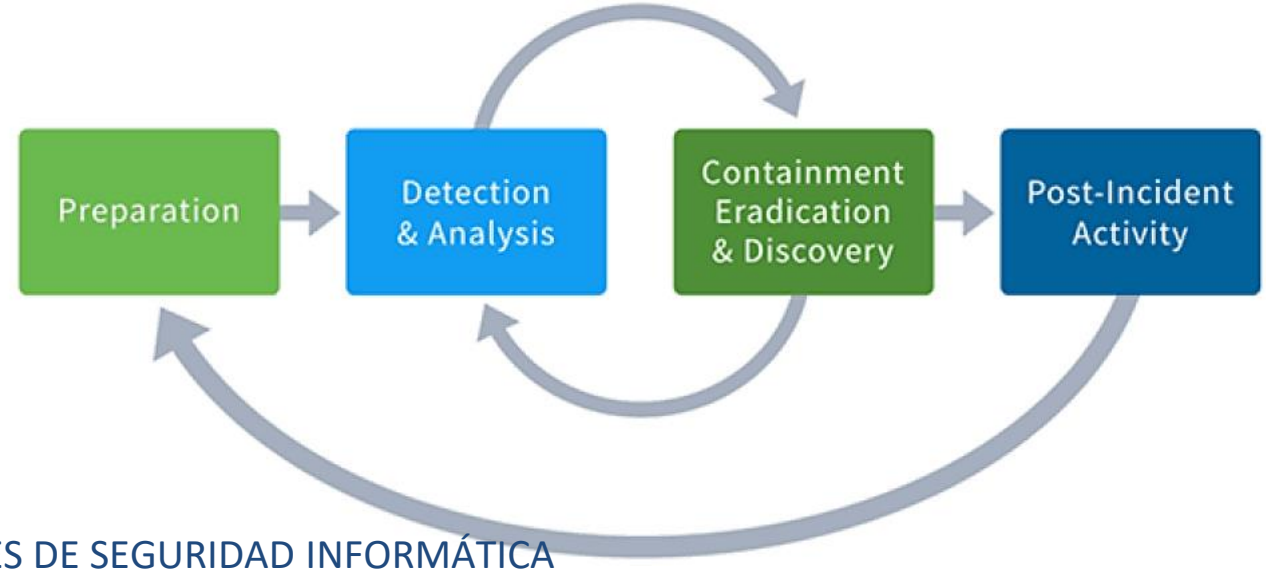
EQUIPO DE RESPUESTA DE INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT)

TODA ORGANIZACIÓN DEBE **DESIGNAR** A UNO O VARIOS **RESPONSABLES** QUE SE ENCARGUEN DE EJECUTAR CON DETALLE LAS TAREAS ASIGNADAS **EN EL PLAN DE RESPUESTA A INCIDENTES** DEFINIDO EN CADA ORGANIZACIÓN.

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

EQUIPO DE RESPUESTA DE INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT)

EL **PLAN DE GESTIÓN DE INCIDENTES,** ELABORADO POR EL RESPONSABLE DE SEGURIDAD INFORMÁTICA, ES ***UN CONJUNTO DE TAREAS Y PROCEDIMIENTOS, JUNTO CON LAS PERSONAS DESIGNADAS, ENCAMINADOS A LA CORRECTA Y ADECUADA GESTIÓN DE INCIDENTES DE SEGURIDAD.***



2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

EQUIPO DE RESPUESTA DE INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT)

EL EQUIPO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD **ESTABLECERÁ**:

- UNA **POLÍTICA GENERAL DE GESTIÓN DE INCIDENTES** EN LA QUE SE DEBERÁ BASAR EL PLAN DE GESTIÓN.
- LOS **PROCEDIMIENTOS A SEGUIR** PARA LA GESTIÓN DE INCIDENTES BASADOS EN LA POLÍTICA E INCLUIDOS EN EL PLAN.
- **RELACIONES ENTRE EL EQUIPO DE RESPUESTA A INCIDENTES Y OTROS GRUPOS** DE LA ORGANIZACIÓN INTERNOS Y EXTERNOS.
- **LAS GUÍAS QUE DEFINAN EL PROCEDIMIENTO A SEGUIR** EN LA COMUNICACIÓN DE LA ORGANIZACIÓN CON TERCEROS EN CASO DE OCURRENCIA DE INCIDENTES.
- **ORGANIZACIÓN DE LOS RESPONSABLES** DE LA GESTIÓN DE RESPUESTA A INCIDENTES Y DEFINICIÓN Y ASIGNACIÓN DE FUNCIONES.

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

EQUIPO DE RESPUESTA DE INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT)

FASES DEL PLAN DE GESTIÓN DE INCIDENTES DE SEGURIDAD:

1. **PREPARACIÓN Y PREVENCIÓN DE INCIDENTES:** ESTABLECIMIENTO DE *MEDIDAS PREVENTIVAS* QUE MINIMICEN EL RIESGO DE INCIDENTES EN LOS SISTEMAS DE LA ORGANIZACIÓN.
2. **DETECCIÓN Y NOTIFICACIÓN:** ESTABLECIMIENTO DE *MEDIDAS DE DETECCIÓN* DE POSIBLES AMENAZAS Y CAPACIDAD DE NOTIFICAR A LOS RESPONSABLES SU DETECCIÓN.
3. **ANÁLISIS PRELIMINAR:** *ANÁLISIS DE LA AMENAZA* PARA VER SI ES UNA AMENAZA REAL O UNA FALSA ALARMA. SI ES REAL, *ANÁLISIS DE LA INCIDENCIA* PARA CONOCER LOS DETALLES Y LOS DAÑOS OCASIONADOS.

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

EQUIPO DE RESPUESTA DE INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT)

FASES DEL PLAN DE GESTIÓN DE INCIDENTES DE SEGURIDAD:

4. **CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN:** ESTABLECIMIENTO DE *MEDIDAS CORRECTIVAS* QUE MINIMICEN LOS DAÑOS OCASIONADOS Y RESTAURAREN EL SISTEMA A SITUACIONES ANTERIORES A LA APARICIÓN DE LA AMENAZA.
5. **INVESTIGACIÓN:** *ANÁLISIS PROFUNDO DE LA INCIDENCIA* PARA CONOCER DETALLADAMENTE SU PROCEDIMIENTO DE ATAQUE Y CÓMO HA PODIDO ACCEDER AL SISTEMA.

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

EQUIPO DE RESPUESTA DE INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT)

FASES DEL PLAN DE GESTIÓN DE INCIDENTES DE SEGURIDAD:

6. **ACTIVIDADES POSTERIORES:** LA INVESTIGACIÓN DEL INCIDENTE SE UTILIZA PARA LLEVAR A CABO UN PROCEDIMIENTO DE *APRENDIZAJE* QUE PERMITA EL ESTABLECIMIENTO DE MEDIDAS CORRECTIVAS QUE IMPIDAN QUE LA AMENAZA SUCEDIDA NO PUEDA VOLVER A ACCEDER A LOS SISTEMAS DE LA ORGANIZACIÓN.

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

EQUIPO DE RESPUESTA DE INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT)

ESQUEMA DEL PROCEDIMIENTO DE GESTIÓN DE INCIDENTES

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

PREPARACIÓN Y PREVENCIÓN DE INCIDENTES

CONSISTE EN DEFINIR UNA SERIE DE MEDIDAS QUE INTENTEN EVITAR LA ENTRADA DE INTRUSIONES AL SISTEMA Y MINIMICEN LOS INCIDENTES EN LA ORGANIZACIÓN.

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

PREPARACIÓN Y PREVENCIÓN DE INCIDENTES

MEDIDAS DE PREPARACIÓN

- **DEFINICIÓN DE LAS POLÍTICAS, NORMAS Y PROCEDIMIENTOS** PARA LA GESTIÓN DE INCIDENTES.
- **DEFINICIÓN DE LOS CRITERIOS DE CLASIFICACIÓN Y PRIORIZACIÓN** DE INCIDENTES.
- **PREPARACIÓN DEL EQUIPO DE RESPUESTA A INCIDENTES** DE SEGURIDAD.
- **ENTRENAMIENTO DEL PERSONAL** DE LA ORGANIZACIÓN.
- **DISEÑO Y FORMALIZACIÓN UN DOCUMENTO** EN EL QUE APAREZCA REFLEJADA LA TOPOLOGÍA Y ARQUITECTURA DE LA RED.
- **CREACIÓN DE LOS PATRONES** DE LAS REDES Y LOS SISTEMAS.

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

PREPARACIÓN Y PREVENCIÓN DE INCIDENTES

MEDIDAS DE PREPARACIÓN

- **ELABORACIÓN DE UN DOCUMENTO** EN EL QUE SE PLASMEN LAS **CONFIGURACIONES DE LOS EQUIPOS** DE LA ORGANIZACIÓN.
- **ACTIVACIÓN DE LOS LOGS** EN LAS APLICACIONES Y SISTEMAS DE LA ORGANIZACIÓN.
- **CENTRALIZACIÓN Y DEFINICIÓN DE UNA POLÍTICA** DE GESTIÓN Y ALMACENAMIENTO DE LOS LOGS.
- **SINCRONIZACIÓN DE LOS RELOJES** DE TODOS LOS EQUIPOS.
- DEFINICIÓN E IMPLEMENTACIÓN DE **SISTEMAS DE** REALIZACIÓN DE **COPIAS DE RESPALDO DE DATOS.**

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

PREPARACIÓN Y PREVENCIÓN DE INCIDENTES

RESULTA NECESARIO LA **UTILIZACIÓN E IMPLANTACIÓN DE HERRAMIENTAS APROPIADAS** QUE PERMITAN LA **DETECCIÓN** DE INCIDENTES, SU **MONITORIZACIÓN**, SU **ANÁLISIS** POSTERIOR, SU **DOCUMENTACIÓN**, ETC.

SE CONSIDERA LA **CATEGORIZACIÓN** DE LOS POSIBLES INCIDENTES QUE PUEDEN OCURRIR. HAY QUE CONSIDERAR DOS **CRITERIOS**:

- **TIPO DE INCIDENTE Y LOS EFECTOS NEGATIVOS PRODUCIDOS O POTENCIALES**
- **ENVERGADURA DE LOS DAÑOS PRODUCIDOS**

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

PREPARACIÓN Y PREVENCIÓN DE INCIDENTES

SEGÚN EL TIPO DE INCIDENTE Y LOS EFECTOS NEGATIVOS PRODUCIDOS O POTENCIALES

TENIENDO EN CUENTA **LOS EFECTOS NEGATIVOS** QUE PRODUCE O PUEDE PRODUCIR UN INCIDENTE SE PUEDE ELABORAR UNA **TABLA DE CATEGORIZACIÓN DE INCIDENTES**:

INCIDENTE	Efectos negativos producidos o potenciales		
	Grave	Moderado	Leve
Incidente 1			
Incidente 2			
Incidente 3			
Incidente 4			
Incidente 5			

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

PREPARACIÓN Y PREVENCIÓN DE INCIDENTES

SEGÚN LA ENVERGADURA DE LOS DAÑOS PRODUCIDOS

TENIENDO EN CUENTA LA **ENVERGADURA DE LOS DAÑOS PRODUCIDOS Y DEL NIVEL DE CRITICIDAD DE LOS RECURSOS** QUE HAN SIDO AFECTADOS POR LA INCIDENCIA, TAMBIÉN SE PUEDE ELABORAR UNA **TABLA DE CLASIFICACIÓN DE INCIDENTES:**

RECURSO	Criticidad de los recursos		
	Alta	Media	Baja
Recurso 1			
Recurso 2			
Recurso 3			
Recurso 4			
Recurso 5			

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

PREPARACIÓN Y PREVENCIÓN DE INCIDENTES

ATENDIENDO A ESTOS DOS CRITERIOS SE ESTABLECERÁ EL **NIVEL DE CRITICIDAD DEL INCIDENTE** DISTINGUIENDO ENTRE MUY GRAVE, GRAVE, MODERADO Y LEVE:

		Criticidad de los recursos		
		Alta	**Media**	**Baja**
Efectos negativos producidos o potenciales	Grave	MUY GRAVE	GRAVE	MODERADO
	Moderado	GRAVE	MODERADO	LEVE
	Leve	MODERADO	LEVE	LEVE

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

PREPARACIÓN Y PREVENCIÓN DE INCIDENTES

SEGÚN LA CRITICIDAD DEL INCIDENTE, SERÁ NECESARIO ESTABLECER TAMBIÉN EL **TIEMPO MÁXIMO** EN EL QUE SE DEBEN **TRATAR LOS INCIDENTES** DESDE EL MOMENTO DE SU DETECCIÓN:

Criticidad del incidente	Tiempo de reacción
LEVE	4 horas
MODERADO	2 horas
GRAVE	30 minutos
MUY GRAVE	10 minutos

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

PREPARACIÓN Y PREVENCIÓN DE INCIDENTES

MEDIDAS DE PREVENCIÓN DE INCIDENTES

- **ANÁLISIS DE RIESGOS** PERIÓDICOS.
- ESTABLECIMIENTO DE **AUDITORÍAS PERIÓDICAS**.
- GESTIÓN EFICAZ DE LAS **ACTUALIZACIONES**.
- ESTABLECIMIENTO DE UN **SISTEMA DE SEGURIDAD EN LA RED**.
- **INCREMENTO** EN TODO LO POSIBLE **DE LA SEGURIDAD DE LOS EQUIPOS** DE LA ORGANIZACIÓN.
- ESTABLECIMIENTOS DE **SISTEMAS DE DETECCIÓN Y PREVENCIÓN** DE CÓDIGOS MALICIOSOS.
- **CONCIENCIACIÓN DEL PERSONAL** DE LA ORGANIZACIÓN.

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

DETECCIÓN Y NOTIFICACIÓN

HAY QUE DISTINGUIR ENTRE **ADVERTENCIAS E INDICADORES**:

- **UNA ADVERTENCIA** ES UNA **SEÑAL** QUE INDICA AL USUARIO QUE **ES POSIBLE** QUE HAYA OCURRIDO UN ACCIDENTE.

  LAS AMENAZAS DE ATAQUES WEB O LAS ALERTAS QUE EMITEN LOS IDS AL REALIZAR UN ESCANEO DE LA RED.

- **UN INDICADOR,** SEÑALA QUE **EL INCIDENTE SE HA PRODUCIDO** O SE ESTÁ PRODUCIENDO.

  DETECCIÓN DE UN VIRUS, EJECUCIÓN LENTA DE LAS APLICACIONES DEL EQUIPO, RALENTIZACIÓN DEL ACCESO A WEBS DE INTERNET, BLOQUEO DE UNA CUENTA DE USUARIO POR INTENTOS FALLIDOS DE ACCESO O CAMBIOS DE CONFIGURACIONES DE APLICACIONES SIN PERMISO DEL USUARIO.

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

DETECCIÓN Y NOTIFICACIÓN

PARA LA FASE DE **DETECCIÓN DE INCIDENTES** LAS ORGANIZACIONES PUEDEN IMPLANTAR **HERRAMIENTAS Y TÉCNICAS DE DETECCIÓN DE INCIDENTES** COMO:

- SISTEMAS IDS/IPS.
- ANTIVIRUS.
- SISTEMAS DE MONITORIZACIÓN DE LA RED.
- ANÁLISIS DE LOS REGISTROS DE AUDITORÍA O LOGS.
- APLICACIONES DE CONTROL DE INTEGRIDAD DE LOS ARCHIVOS Y DATOS.

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

DETECCIÓN Y NOTIFICACIÓN

PARA LA **NOTIFICACIÓN DEL INCIDENTE**, LAS ORGANIZACIONES DEBEN **DISEÑAR UN PROCESO DE NOTIFICACIÓN** EN EL QUE SE INCLUYAN LAS PAUTAS, PROCEDIMIENTOS Y MÉTODOS DE NOTIFICACIÓN QUE HAY QUE REALIZAR EN CUANTO SE DETECTA UN INCIDENTE.

DEBE DEFINIRSE **A QUIÉN HAY QUE NOTIFICAR** EL INCIDENTE, ATENDIENDO AL TIPO Y SU RELEVANCIA.

LOS INTERESADOS A LOS QUE SE LES DEBE NOTIFICAR PUEDEN SER EL MISMO PERSONAL DE INFORMÁTICA, EL RESPONSABLE DE SEGURIDAD, LOS DUEÑOS DE LA INFORMACIÓN AFECTADA, ALTOS DIRECTIVOS DE LA ORGANIZACIÓN, ETC.

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

ANÁLISIS PRELIMINAR

LA FASE DE ANÁLISIS PRELIMINAR DEL POSIBLE INCIDENTE CONSISTE EN **REALIZAR UN ANÁLISIS** DE LOS INDICADORES Y ADVERTENCIAS DISPONIBLES PARA **DETECTAR SI REALMENTE ES UN INCIDENTE DE SEGURIDAD O ES UNA FALSA ALARMA**.

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

ANÁLISIS PRELIMINAR

EN CASO DE SER UN INCIDENTE REAL SE DEBE SEGUIR **UN PROCESO DE RECOLECCIÓN** DE INFORMACIÓN PARA **ANALIZAR**:

- ***EL ALCANCE DEL INCIDENTE:*** REDES, EQUIPOS, SISTEMAS Y APLICACIONES AFECTADOS.
- ***CAUSA***. *QUÉ* HA SIDO LO QUE HA ORIGINADO EL INCIDENTE.
- ***IMPACTO DEL INCIDENTE*** EN LAS ACTIVIDADES, SERVICIOS Y PROCESOS DE LA ORGANIZACIÓN.
- ***CÓMO HA OCURRIDO*** O ESTÁ OCURRIENDO EL INCIDENTE EN CUANTO A MÉTODOS Y HERRAMIENTAS UTILIZADAS, VULNERABILIDADES DETECTADAS Y EXPLOTADAS, ETC.

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

ANÁLISIS PRELIMINAR

EL **ALCANCE** DEL INCIDENTE SE PUEDE DETERMINAR **TENIENDO EN CUENTA ASPECTOS** COMO:

- CANTIDAD DE **EQUIPOS** COMPROMETIDOS.
- CANTIDAD DE **REDES A**FECTADAS.
- **NIVEL DE PRIVILEGIO** ALCANZADO POR LA INTRUSIÓN.
- **NIVEL DE RIESGO** DE LAS **APLICACIONES CRÍTICAS**.
- **NIVEL DE RIESGO** GENERAL DE LOS **EQUIPOS** Y DE **LA RED**.
- **NIVEL DE CONOCIMIENTO DE LA VULNERABILIDAD EXPLOTADA** POR LA INTRUSIÓN.
- **ANÁLISIS DE LOS DEMÁS EQUIPOS** PARA COMPROBAR SI TIENEN LA MISMA VULNERABILIDAD.

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

ANÁLISIS PRELIMINAR

CUANDO SE HA CLASIFICADO EL INCIDENTE COMO REAL, SE PUEDEN UTILIZAR VARIOS **MÉTODOS Y FORMAS DE RECOLECTAR INFORMACIÓN** PARA OBTENER UN CONOCIMIENTO MÁS PROFUNDO Y DETALLADO DEL INCIDENTE Y DE SU ALCANCE:

- **INDAGACIÓN A LOS ADMINISTRADORES** DEL SISTEMA.
- **INDAGACIÓN AL PERSONAL** QUE FORMA PARTE DE LA ORGANIZACIÓN.
- REVISIÓN DE LOS **REPORTES** DE LOS SISTEMAS Y HERRAMIENTAS IDS.
- REVISIÓN DE LOS **LOGS** REFERENTES A LAS COMUNICACIONES Y SISTEMAS.
- REVISIÓN DE LA **TOPOLOGÍA Y ARQUITECTURA DE LA RED**.
- REVISIÓN DE LAS **LISTAS DE ACCESO A LA RED.**

2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD

ANÁLISIS PRELIMINAR

ALGUNOS DE LOS **DATOS RECOLECTADOS** A TRAVÉS DEL PROCESO DE RECOGIDA DE INFORMACIÓN PUEDEN SER:

- INFORMACIÓN DE LOS **SUCESOS ANORMALES** EN LOS SISTEMAS Y EN LAS ACTIVIDADES RUTINARIAS.
- DETECCIÓN DE **ACTIVIDADES ANORMALES**.
- CONOCIMIENTO DE LOS **DETALLES CONCRETOS** DEL INCIDENTE.
- DETECCIÓN DE **CAMBIOS NO AUTORIZADOS**.

CONTENIDOS

1. INTRODUCCIÓN
2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD
3. **EXPOSICIÓN DE LAS DISTINTAS TÉCNICAS Y HERRAMIENTAS UTILIZADAS PARA EL ANÁLISIS Y CORRELACIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD**
4. PROCESO DE VERIFICACIÓN DE LA INTRUSIÓN
5. NATURALEZA Y FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES TIPO CERT NACIONALES E INTERNACIONALES

3. EXPOSICIÓN DE LAS DISTINTAS TÉCNICAS Y HERRAMIENTAS UTILIZADAS PARA EL ANÁLISIS Y CORRELACIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD

UNO DE LOS CONCEPTOS EN LOS QUE ESTÁ BASADA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN ES **EL ANÁLISIS Y LA GESTIÓN DE LOGS Y LA CORRELACIÓN DE EVENTOS DE SEGURIDAD.**

LAS **HERRAMIENTAS DE CORRELACIÓN DE EVENTOS** PERMITEN LLEVAR A CABO UNA GESTIÓN MÁS EFICIENTE DE TODOS LOS SISTEMAS, HERRAMIENTAS Y APLICACIONES CRÍTICAS MEDIANTE SU MONITORIZACIÓN.

ADEMÁS, ***LA GESTIÓN DE EVENTOS DE SEGURIDAD FACILITA LA DETECCIÓN DE POSIBLES VULNERABILIDADES Y AMENAZAS CON EL FIN DE CONSEGUIR MINIMIZAR LOS RIESGOS DE INTRUSIONES***.

3. EXPOSICIÓN DE LAS DISTINTAS TÉCNICAS Y HERRAMIENTAS UTILIZADAS PARA EL ANÁLISIS Y CORRELACIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD

LAS **HERRAMIENTAS DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD** SON UN CONJUNTO DE PRODUCTOS **CUYA FUNCIÓN ES LA GESTIÓN DE EVENTOS O INCIDENTES DE SEGURIDAD** EN CUALQUIERA DE SUS FASES, TANTO ANTES, COMO DURANTE O DESPUÉS DE LA OCURRENCIA DEL INCIDENTE.

SE ENCARGAN DE RECOGER, COTEJAR Y ELABORAR INFORMES CON LOS DATOS FACILITADOS POR LOS LOGS.

TAMBIÉN PERMITEN **LLEVAR A CABO UN TRATAMIENTO ORGANIZADO DE LOS INCIDENTES** CON EL FIN DE RESOLVERLOS EN EL MENOR TIEMPO POSIBLE INTENTANDO MINIMIZAR LOS DAÑOS OCASIONADOS.

3. EXPOSICIÓN DE LAS DISTINTAS TÉCNICAS Y HERRAMIENTAS UTILIZADAS PARA EL ANÁLISIS Y CORRELACIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD

UN **SISTEMA DE ANÁLISIS Y CORRELACIÓN DE EVENTOS** ADECUADO DEBE PERMITIR:

- LA **DETERMINACIÓN EN TIEMPO REAL DE LA PROBABILIDAD DE MATERIALIZARSE UNA AMENAZA** EN UN MOMENTO CONCRETO.
- LA **DETECCIÓN A TIEMPO REAL DEL INICIO DE UN ATAQUE**, EMITIENDO ALERTAS CON LA MENOR DEMORA POSIBLE.
- EL **CONOCIMIENTO DEL ÉXITO O FRACASO DE UN ATAQUE** Y DE SU **IMPACTO REAL** SOBRE EL SISTEMA.
- LA **DETERMINACIÓN** DE LOS **PATRONES DE MATERIALIZACIÓN DE LAS AMENAZAS** PARA SER UTILIZADOS EN LA IMPLANTACIÓN DE NUEVAS MEDIDAS DE SEGURIDAD.

3. EXPOSICIÓN DE LAS DISTINTAS TÉCNICAS Y HERRAMIENTAS UTILIZADAS PARA EL ANÁLISIS Y CORRELACIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD

ENTRE LAS TÉCNICAS Y ***HERRAMIENTAS UTILIZADAS PARA EL ANÁLISIS Y CORRELACIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD*** SE DISTINGUEN **TRES TIPOS DE SISTEMAS**:

- SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN O **SIM (SECURITY INFORMATION MANAGEMENT).**
- SISTEMAS DE GESTIÓN DE EVENTOS O **SEM (SECURITY EVENT MANAGEMENT).**
- SISTEMAS DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD O **SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT).**

3. EXPOSICIÓN DE LAS DISTINTAS TÉCNICAS Y HERRAMIENTAS UTILIZADAS PARA EL ANÁLISIS Y CORRELACIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD

SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SIM)

SON SISTEMAS PARA LA RECOGIDA, CORRELACIÓN Y EL ANÁLISIS DE LA INFORMACIÓN DE SEGURIDAD EN DIFERIDO, NO A TIEMPO REAL.

LO REALIZAN CREANDO UNA BASE DE DATOS INDEXADA BASADA EN LOS DATOS OBTENIDOS EN LAS SUPERVISIONES REALIZADAS A LOS EQUIPOS Y DISPOSITIVOS.

3. EXPOSICIÓN DE LAS DISTINTAS TÉCNICAS Y HERRAMIENTAS UTILIZADAS PARA EL ANÁLISIS Y CORRELACIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD

SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SIM)

ENTRE SUS **FUNCIONES PRINCIPALES** CABE DESTACAR:

- **RECOGIDA, ORDENACIÓN Y CORRELACIÓN** DE INFORMACIÓN DE LA RED.
- **AUTOMATIZACIÓN Y MONITORIZACIÓN DE LOS EVENTOS** DE SISTEMAS Y DISPOSITIVOS DE SEGURIDAD.
- **CENTRALIZACIÓN, CORRELACIÓN Y PRIORIZACIÓN** DE EVENTOS CON EL FIN DE:
  - ESTANDARIZAR LOS EVENTOS.
  - REDUCIR LO MÁXIMO POSIBLE EL TIEMPO DE DETECCIÓN DE ATAQUES Y VULNERABILIDADES EN LA RED.
  - MINIMIZAR LA INFORMACIÓN A PROCESAR PARA OBTENER MEJORAS DE RENDIMIENTO.

3. EXPOSICIÓN DE LAS DISTINTAS TÉCNICAS Y HERRAMIENTAS UTILIZADAS PARA EL ANÁLISIS Y CORRELACIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD

SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SIM)

LOS **SIM SE UTILIZAN** SOBRE TODO PARA:

- ADMINISTRAR LA INFRAESTRUCTURA DE LA RED Y DE LOS ACTIVOS DE LA ORGANIZACIÓN.
- CENTRALIZAR Y MONITORIZAR LOS COMPONENTES DE LA INFRAESTRUCTURA DE SEGURIDAD DE LA ORGANIZACIÓN.
- ANALIZAR CON MAYOR FACILIDAD LA INFORMACIÓN SUMINISTRADA POR LOS COMPONENTES DE SEGURIDAD.
- PREDECIR Y PRONOSTICAR AMENAZAS.
- CORRELACIONAR EVENTOS DE SEGURIDAD.
- DETECTAR, IDENTIFICAR Y EMITIR REPORTES DE EVENTOS DE SEGURIDAD.
- REALIZAR UN ANÁLISIS FORENSE DE LOS EVENTOS.
- ESTABLECER POLÍTICAS DE SEGURIDAD MÁS ADECUADAS.

3. EXPOSICIÓN DE LAS DISTINTAS TÉCNICAS Y HERRAMIENTAS UTILIZADAS PARA EL ANÁLISIS Y CORRELACIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD

SISTEMAS DE GESTIÓN DE EVENTOS (SEM)

SE ENCARGAN DE MONITORIZAR Y GESTIONAR LOS EVENTOS PRÁCTICAMENTE A TIEMPO REAL.

SU FUNCIÓN PRINCIPAL CONSISTE EN **RECOGER LOS DATOS DE LOS EVENTOS DE SEGURIDAD PRODUCIDOS** EN LOS DISTINTOS EQUIPOS, SISTEMAS Y DISPOSITIVOS CON EL FIN DE REALIZAR **ANÁLISIS A TIEMPO REAL Y RESPONDER** EN EL MENOR TIEMPO POSIBLE.

3. EXPOSICIÓN DE LAS DISTINTAS TÉCNICAS Y HERRAMIENTAS UTILIZADAS PARA EL ANÁLISIS Y CORRELACIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD

SISTEMAS DE GESTIÓN DE EVENTOS (SEM)

LOS **BENEFICIOS** DE LOS **SEM** SON:

- ACCESO A LOS REGISTROS A TRAVÉS DE UNA **INTERFAZ CENTRAL** CONSISTENTE.
- **ALMACENAMIENTO SEGURO DE LOS REGISTROS**, MANTENIENDO SU INTEGRIDAD.
- **REPRESENTACIÓN GRÁFICA DE LA ACTIVIDAD** PARA UNA ELABORACIÓN DE INFORMES MÁS SENCILLA, VISUAL Y PRÁCTICA.
- **ACTIVACIÓN DE ALERTAS** PROGRAMADAS.
- **GESTIÓN DE EVENTOS** DE VARIOS SISTEMAS OPERATIVOS.
- **RECUPERACIÓN DE REGISTROS** ANTE BLOQUEOS DEL SISTEMA O ELIMINACIÓN INESPERADA DE REGISTROS.

3. EXPOSICIÓN DE LAS DISTINTAS TÉCNICAS Y HERRAMIENTAS UTILIZADAS PARA EL ANÁLISIS Y CORRELACIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD

SISTEMAS DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIEM)

SON UNA MEZCLA DE LAS HERRAMIENTAS **SIM** Y **SEM**.

RECOGEN LOS LOGS DE LOS SISTEMAS MONITORIZADOS, LOS ALMACENAN A LARGO PLAZO, AGREGAN Y CORRELACIONAN EN TIEMPO REAL LA INFORMACIÓN RECIBIDA PARA UNA DETECCIÓN Y ESTABLECIMIENTO DE MEDIDAS MÁS EFICAZ, MINIMIZANDO LOS DAÑOS OCASIONADOS.

3. EXPOSICIÓN DE LAS DISTINTAS TÉCNICAS Y HERRAMIENTAS UTILIZADAS PARA EL ANÁLISIS Y CORRELACIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD

SISTEMAS DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIEM)

PERMITEN UNA GESTIÓN DE INCIDENTES DE SEGURIDAD MÁS GLOBAL Y ENTRE SUS **FUNCIONES PRINCIPALES** DESTACAN:

- DETECCIÓN DE ANOMALÍAS Y AMENAZAS.
- ANÁLISIS DE TODAS LAS FASES DEL INCIDENTE.
- CAPTURA TOTAL DE LOS PAQUETES DE LA RED.
- CONOCIMIENTO DEL COMPORTAMIENTO DEL USUARIO Y SU CONTEXTO.
- CUMPLIMIENTO DE NUEVAS NORMATIVAS.

3. EXPOSICIÓN DE LAS DISTINTAS TÉCNICAS Y HERRAMIENTAS UTILIZADAS PARA EL ANÁLISIS Y CORRELACIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD

SISTEMAS DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIEM)

FUNCIONES:

- ADMINISTRACIÓN MÁS EFECTIVA DEL RIESGO GRACIAS A INFORMACIÓN OBTENIDA COMO:
  - TOPOLOGÍA Y ARQUITECTURA DE LA RED.
  - VULNERABILIDADES DETECTADAS.
  - PARÁMETROS DE CONFIGURACIÓN DEL EQUIPO Y DE LOS DISPOSITIVOS.
  - ANÁLISIS DE FALLOS.
  - PRIORIZACIÓN DE VULNERABILIDADES.
  - CORRELACIÓN AVANZADA Y PROFUNDA DE LOS EVENTOS.

3. EXPOSICIÓN DE LAS DISTINTAS TÉCNICAS Y HERRAMIENTAS UTILIZADAS PARA EL ANÁLISIS Y CORRELACIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD

SISTEMAS DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIEM)

LAS HERRAMIENTAS **SIM, SEM Y SIEM** DISPONIBLES EN EL MERCADO SON DE LO MÁS VARIADAS.

AUN ASÍ, LAS HERRAMIENTAS **SIEM** GENERALMENTE SUELEN DECANTARSE POR DISPONER MÁS HERRAMIENTAS **SIM** O **SEM** ATENDIENDO A LAS FUNCIONALIDADES QUE PRETENDEN CUBRIR.

EN EL MOMENTO DE ELEGIR UNA HERRAMIENTA, LAS ORGANIZACIONES DEBEN REALIZAR UN ANÁLISIS PREVIO DE NECESIDADES Y PRIORIDADES PARA ELEGIR LA HERRAMIENTA MÁS ADECUADA Y PERTINENTE.

3. EXPOSICIÓN DE LAS DISTINTAS TÉCNICAS Y HERRAMIENTAS UTILIZADAS PARA EL ANÁLISIS Y CORRELACIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD

SISTEMAS DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIEM)

LISTA DE HERRAMIENTAS SIEM:

EXABEAM FUSION, MICROSOFT SENTINEL, GRAYLOG, IBM QRADAR, LOGRHYTHM, SOLARWINDS, SPLUNK, ELASTIC SECURITY, INSIGHTSIDR, SUMO LOGIC, NETWITNESS, ALIENVAULT OSSIM

CONTENIDOS

1. INTRODUCCIÓN
2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD
3. EXPOSICIÓN DE LAS DISTINTAS TÉCNICAS Y HERRAMIENTAS UTILIZADAS PARA EL ANÁLISIS Y CORRELACIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD
4. **PROCESO DE VERIFICACIÓN DE LA INTRUSIÓN**
5. NATURALEZA Y FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES TIPO CERT NACIONALES E INTERNACIONALES

4. PROCESO DE VERIFICACIÓN DE LA INTRUSIÓN

VAMOS A DESCRIBIR EL **PROCESO DE VERIFICACIÓN DE LA INTRUSIÓN**, PERO PARA ELLO ES FUNDAMENTAL COMENTAR ANTES LAS **FASES PREVIAS** PARA UNA MAYOR COMPRENSIÓN DEL PROCESO:

- **CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN ANTE INCIDENTES DE SEGURIDAD**
- **ELABORACIÓN DEL INFORME FINAL DEL INCIDENTE**
- **DOCUMENTACIÓN DEL INCIDENTE**

4. PROCESO DE VERIFICACIÓN DE LA INTRUSIÓN

CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN ANTE INCIDENTES DE SEGURIDAD

UNA VEZ VERIFICADO QUE UN INCIDENTE ES REAL Y CONCLUIDO EL PROCESO DE RECOLECCIÓN DE INFORMACIÓN, PARA CONOCER CON MÁS PROFUNDIDAD SUS DETALLES SE PROSIGUE CON LA FASE DE **CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN**:

- LA **CONTENCIÓN** *ES EVITAR QUE EL INCIDENTE SIGA PRODUCIENDO MÁS DAÑOS*
- LA **ERRADICACIÓN** *ES ELIMINAR AQUELLO QUE PROVOCÓ EL INCIDENTE Y TODO EL RASTRO DE LOS DAÑOS PRODUCIDOS*
- LA **RECUPERACIÓN** *ES DEVOLVER LOS SISTEMAS, DISPOSITIVOS Y EQUIPOS A SU ESTADO ORIGINAL ANTES DE PRODUCIRSE EL INCIDENTE.*

4. PROCESO DE VERIFICACIÓN DE LA INTRUSIÓN

ELABORACIÓN DEL INFORME FINAL DEL INCIDENTE

CUANDO YA SE HA ELIMINADO EL INCIDENTE Y SE HA PODIDO VOLVER A LA SITUACIÓN ORIGINAL, LO SIGUIENTE QUE DEBE REALIZARSE ES EL **PROCESO DE INVESTIGACIÓN DEL INCIDENTE** Y LA REALIZACIÓN DE ACTIVIDADES POSTERIORES (COMO LA DEFINICIÓN DE NUEVAS MEDIDAS DE SEGURIDAD) CON LA INFORMACIÓN OBTENIDA EN EL PROCESO DE INVESTIGACIÓN.

EN LA INVESTIGACIÓN DEL INCIDENTE SE DEBE REALIZAR LA VERIFICACIÓN DE LA INTRUSIÓN MEDIANTE LA ELABORACIÓN DE UN **INFORME FINAL** QUE DEBER CONTENER, COMO MÍNIMO, LOS ASPECTOS QUE SE REFLEJAN EN LA TABLA SIGUIENTE:

4. PROCESO DE VERIFICACIÓN DE LA INTRUSIÓN

ELABORACIÓN DEL INFORME FINAL DEL INCIDENTE

Aspectos a reflejar en el informe	Actividades a realizar
Análisis de las causas y consecuencias del incidente	Revisión exhaustiva de los logs de los equipos, sistemas y dispositivos afectados por el incidente.
	Análisis de las consecuencias que hayan podido afectar a terceros.
	Análisis de la información del incidente compartida con terceros.
	Cuantificación del coste de los daños provocados por la intrusión en la organización en cuanto a daño en equipos, aplicaciones afectadas, información perdida, personal técnico especializado contratado, etc.
	Estudio de la documentación elaborada por el equipo de respuesta a incidentes de seguridad.
	Evaluación y control de las posibles acciones legales que se hayan podido emprender por el incidente.

Aspectos a reflejar en el informe	Actividades a realizar
Evaluación de la toma de decisiones y de las actuaciones llevadas a cabo por el equipo de respuesta a incidentes	Rapidez de respuesta en decisiones y medidas tomadas por el equipo de respuesta a incidentes.
	Personal integrante, formación recibida, organización y papeles asignados en el equipo de respuesta a incidentes.
	Implementación de nuevas herramientas necesarias para evitar futuros incidentes.
	Evaluación de los procedimientos y de las herramientas técnicas utilizadas en la respuesta al incidente: - Los procedimientos que no hayan funcionado deben rediseñarse. - Se deben adoptar medidas correctivas que mejoren la respuesta ante futuras incidencias.
Análisis de las políticas de seguridad	Revisión de las políticas de seguridad de la información para detectar fallos y redefinir aquellas pautas ineficientes.
Análisis de directrices de la organización	Revisión de las directrices actuales de la organización e implantación de nuevas directrices para reforzar su nivel de seguridad.

4. PROCESO DE VERIFICACIÓN DE LA INTRUSIÓN

ELABORACIÓN DEL INFORME FINAL DEL INCIDENTE

CON LA EVALUACIÓN Y ANÁLISIS DE TODOS LOS ASPECTOS REFLEJADOS EN EL INFORME DE VERIFICACIÓN DEL INCIDENTE YA **SE PUEDE OBTENER UNA IMAGEN GLOBAL** DE **POR QUÉ SUCEDIÓ** LA INTRUSIÓN, **QUÉ ES LO QUE HA QUEDADO AFECTADO**, **CÓMO SE HA ACTUADO** AL RESPECTO Y **QUÉ HAY QUE MODIFICAR PARA QUE NO VUELVA A OCURRIR**.

DE ESTE MODO SE REALIZA UN **PROCESO DE APRENDIZAJE DEL INCIDENTE** PARA QUE EN FUTURAS INTRUSIONES LA RESPUESTA SEA MÁS RÁPIDA Y EFECTIVA Y LOS DAÑOS OCASIONADOS SEAN LO MÁS REDUCIDOS POSIBLE.

4. PROCESO DE VERIFICACIÓN DE LA INTRUSIÓN

DOCUMENTACIÓN DEL INCIDENTE

PARA QUE EL PROCESO DE APRENDIZAJE DEL INCIDENTE SEA MÁS EFECTIVO Y NO SE OLVIDEN DETALLES **SE RECOMIENDA LLEVAR A CABO UNA DOCUMENTACIÓN DEL INCIDENTE** COMENTANDO SU EVOLUCIÓN EN TODAS LAS FASES.

HAY QUE DOCUMENTAR DE UN MODO CONCRETO Y PRECISO LOS ASPECTOS MÁS FUNDAMENTALES Y QUE NO DEBEN OLVIDARSE UNA VEZ SOLUCIONADO EL INCIDENTE.

4. PROCESO DE VERIFICACIÓN DE LA INTRUSIÓN

DOCUMENTACIÓN DEL INCIDENTE

MÁS CONCRETAMENTE, **LA DOCUMENTACIÓN DEL INCIDENTE DE SEGURIDAD DEBE INCLUIR**:

- **REPORTE DEL INCIDENTE** EN EL QUE SE DEBE ESPECIFICAR:
  - TIPO DE INCIDENTE.
  - HECHOS OCURRIDOS.
  - DAÑOS OCASIONADOS.
- **ESTADO ACTUAL DEL INCIDENTE** (FECHANDO LAS DISTINTAS ETAPAS POR LAS QUE HA IDO PASANDO EL INCIDENTE).
- **CONCLUSIONES DEL ANÁLISIS.**
- **ACCIONES Y MEDIDAS TOMADAS** PARA ERRADICAR EL INCIDENTE Y RESTAURAR LOS EQUIPOS AFECTADOS.

4. PROCESO DE VERIFICACIÓN DE LA INTRUSIÓN

DOCUMENTACIÓN DEL INCIDENTE

- **EVIDENCIAS OBTENIDAS** EN EL PROCESO DE ANÁLISIS POSTERIOR.
- **PERSONAS INVOLUCRADAS,** TANTO A NIVEL INTERNO DE LA EMPRESA COMO A NIVEL EXTERNO (TERCEROS).
- **ACCIONES FUTURAS Y RECOMENDACIONES** PARA AUMENTAR EL NIVEL DE SEGURIDAD Y EVITAR INCIDENCIAS SIMILARES EN PRÓXIMAS OCASIONES.

UNA **ADECUADA DOCUMENTACIÓN** DE LOS INCIDENTES **FACILITA EL ESTUDIO E INVESTIGACIÓN POSTERIOR**.

ES INFORMACIÓN MUY DELICADA QUE AFECTA DIRECTAMENTE A LOS RECURSOS DE UNA ORGANIZACIÓN, POR LO QUE **DEBERÁ ESTAR BAJO PROTECCIÓN PARA EVITAR ACCESOS NO AUTORIZADOS.**

CONTENIDOS

1. INTRODUCCIÓN
2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD
3. EXPOSICIÓN DE LAS DISTINTAS TÉCNICAS Y HERRAMIENTAS UTILIZADAS PARA EL ANÁLISIS Y CORRELACIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD
4. PROCESO DE VERIFICACIÓN DE LA INTRUSIÓN
5. **NATURALEZA Y FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES TIPO CERT NACIONALES E INTERNACIONALES**

5. NATURALEZA Y FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES TIPO CERT NACIONALES E INTERNACIONALES

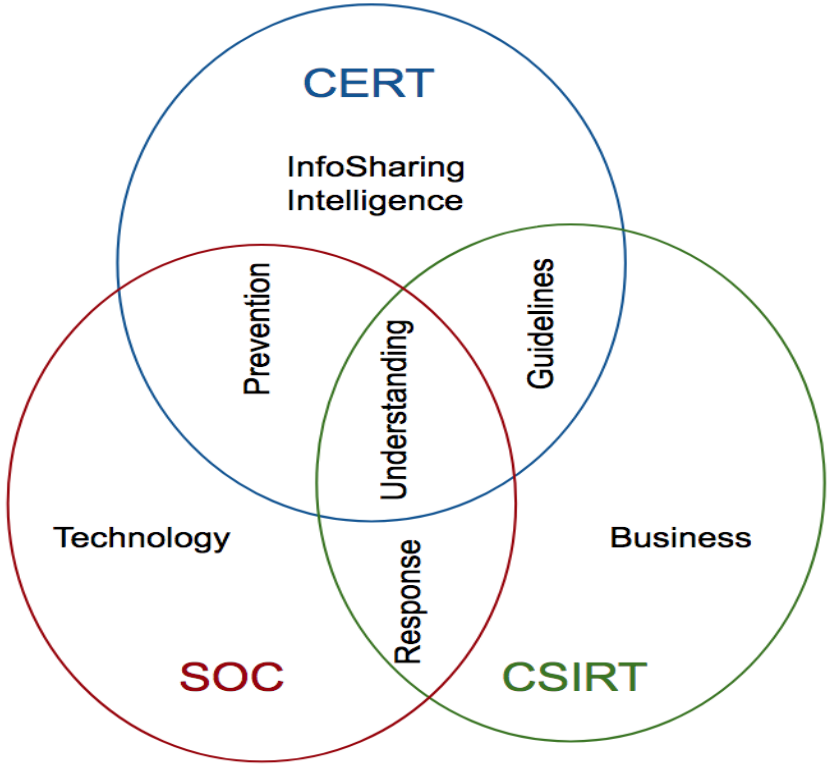
ACTUALMENTE, **LAS TECNOLOGÍAS DE LA INFORMACIÓN** (TIC) SE HAN DESARROLLADO DE TAL MODO QUE **SE HAN CONVERTIDO EN** UNA DE LAS **HERRAMIENTAS** MÁS **BÁSICAS PARA LA GESTIÓN** Y EL BUEN FUNCIONAMIENTO **DE LAS ORGANIZACIONES** HASTA EL PUNTO DE **RESULTAR IMPRESCINDIBLES**.

LAS TIC SE HAN IDO DESARROLLANDO A UN RITMO TAN VELOZ QUE **ES NECESARIO AUMENTAR LAS MEDIDAS PARA COMBATIR PROBLEMAS DE SEGURIDAD, ATAQUES, INTRUSIONES Y PROBLEMAS DE VULNERABILIDADES** QUE CADA VEZ SON MÁS SOFISTICADOS Y DAÑINOS.

5. NATURALEZA Y FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES TIPO CERT NACIONALES E INTERNACIONALES

ORGANISMOS CERT/CSIRT

PARA COMBATIR MÁS EFICAZMENTE LAS AMENAZAS A LA SEGURIDAD DE LOS SISTEMAS INFORMÁTICOS **SE HAN CREADO DISTINTOS ORGANISMOS PARA REALIZAR TAREAS DE INFORMACIÓN Y CONCIENCIACIÓN A LOS GOBIERNOS, EMPRESAS Y USUARIOS** PARA CONSEGUIR CONTENER AMENAZAS Y REDUCIR LOS DAÑOS QUE PUEDEN OCASIONAR.



5. NATURALEZA Y FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES TIPO CERT NACIONALES E INTERNACIONALES

ORGANISMOS CERT/CSIRT

LOS **CERT (COMPUTER EMERGENCY RESPONSE TEAM O EQUIPO DE RESPUESTA ANTE EMERGENCIAS INFORMÁTICAS)** SON *CENTROS DE RESPUESTA A INCIDENTES DE SEGURIDAD EN TECNOLOGÍAS DE INFORMACIÓN FORMADOS POR EXPERTOS ENCARGADOS DE DISEÑAR MEDIDAS PREVENTIVAS Y REACTIVAS ANTE INCIDENTES DE SEGURIDAD*.

5. NATURALEZA Y FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES TIPO CERT NACIONALES E INTERNACIONALES

ORGANISMOS CERT/CSIRT

POCO DESPUÉS DE LA CREACIÓN DE LOS **CERT**, SE COMENZÓ A HABLAR DE LOS **CSIRT (COMPUTER SECURITY INCIDENT RESPONSE TEAM O EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA)**, PARA COMPLETAR EL CONCEPTO DE **CERT** Y **OFRECER COMO VALOR AÑADIDO LOS SERVICIOS PREVENTIVOS Y DE GESTIÓN DE SEGURIDAD**, ASUMIENDO EL RESTO DE LAS ACTIVIDADES CLAVE DE LA GESTIÓN DE LA SEGURIDAD.

5. NATURALEZA Y FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES TIPO CERT NACIONALES E INTERNACIONALES

ORGANISMOS CERT/CSIRT

DE LOS **CERT/CSIRT** HAY QUE DESTACAR TRES TIPOS DE **SERVICIOS**:

- **SERVICIOS REACTIVOS**
- **SERVICIOS PROACTIVOS**
- **SERVICIOS DE GESTIÓN DE CALIDAD DE LA SEGURIDAD**

5. NATURALEZA Y FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES TIPO CERT NACIONALES E INTERNACIONALES

ORGANISMOS CERT/CSIRT

SERVICIOS REACTIVOS

ELABORACIÓN DE INFORMES DE EQUIPOS, SISTEMAS Y DISPOSITIVOS AFECTADOS POR AMENAZAS, CÓDIGOS MALICIOSOS, VULNERABILIDADES Y OTROS EVENTOS DE SEGURIDAD DETECTADOS EN LOS REGISTROS.

ESTAS ACTIVIDADES SON LAS FUNCIONES PRINCIPALES DE LOS **CERT Y CSIRT**.

5. NATURALEZA Y FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES TIPO CERT NACIONALES E INTERNACIONALES

ORGANISMOS CERT/CSIRT

SERVICIOS REACTIVOS

LOS **SERVICIOS PRINCIPALES** SON:

- ANÁLISIS DE LA SITUACIÓN.
- ELABORACIÓN DE RECOMENDACIONES PARA CONTROLAR LA SITUACIÓN ANTE INCIDENTES.
- DISEÑO DE CONTRAMEDIDAS DE SEGURIDAD PARA REDUCIR EL RIESGO DE FUTURAS AMENAZAS.

5. NATURALEZA Y FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES TIPO CERT NACIONALES E INTERNACIONALES

ORGANISMOS CERT/CSIRT

SERVICIOS PROACTIVOS

SERVICIOS DE *ASISTENCIA E INFORMACIÓN PARA AYUDAR A PREVENIR, PREPARAR Y PROTEGER LOS SISTEMAS, EQUIPOS Y DISPOSITIVOS DE LOS USUARIOS* PARA REDUCIR EL RIESGO DE PRODUCCIÓN DE AMENAZAS E INCIDENTES EN UN FUTURO.

SERVICIOS DE GESTIÓN DE CALIDAD DE LA SEGURIDAD

SERVICIOS INDEPENDIENTES DE LA GESTIÓN DE INCIDENTES ENCARGADOS DE BUSCAR HERRAMIENTAS Y MEDIDAS QUE MEJOREN LA CALIDAD DE LA SEGURIDAD INFORMÁTICA. SE BASAN SOBRE TODO EN ACTIVIDADES DE CONCIENCIACIÓN Y EDUCACIÓN DE LOS USUARIOS.

5. NATURALEZA Y FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES TIPO CERT NACIONALES E INTERNACIONALES

ORGANISMOS CERT/CSIRT

EN CUANTO A **FUNCIONES** DE ESTOS ORGANISMOS CABE DESTACAR:

- AYUDAR AL PÚBLICO OBJETIVO A PREVENIR Y ATENUAR INCIDENTES GRAVES DE SEGURIDAD.
- AYUDAR A PROTEGER INFORMACIONES Y DATOS DE GRAN VALOR.
- COORDINAR CENTRALIZADAMENTE LA SEGURIDAD DE LA INFORMACIÓN.
- APOYAR Y ASISTIR A LOS USUARIOS PARA QUE EL PROCESO DE RECUPERACIÓN ANTE INCIDENTES DE SEGURIDAD SEA LO MÁS LEVE POSIBLE.
- DIRIGIR CENTRALIZADAMENTE LA RESPUESTA ANTE INCIDENTES DE SEGURIDAD.

5. NATURALEZA Y FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES TIPO CERT NACIONALES E INTERNACIONALES

ORGANISMOS CERT/CSIRT

PARA DESEMPEÑAR SUS FUNCIONES LOS **CSIRT/CERT LAS LLEVAN A CABO MEDIANTE**:

- EL MANTENIMIENTO DE UNA **BASE DE DATOS DE VULNERABILIDADES** DE SEGURIDAD PARA CONSULTA, SEGUIMIENTO Y REGISTRO HISTÓRICO.
- EL MANTENIMIENTO DE UNA **BASE DE DATOS DE INCIDENTES** DE SEGURIDAD DE LAS ORGANIZACIONES INTEGRANTES.
- PROVISIÓN DE UN **SERVICIO DE ASESORAMIENTO** ESPECIALIZADO EN SEGURIDAD DE LA INFORMACIÓN.
- MANTENIMIENTO DE **CONTACTOS CON OTROS CSIRT/CERT** DEL MUNDO Y SUS ORGANIZACIONES PARA INTERCAMBIAR INFORMACIÓN.

5. NATURALEZA Y FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES TIPO CERT NACIONALES E INTERNACIONALES

ORGANISMOS CERT/CSIRT

EN ESPAÑA, EL SECTOR PÚBLICO, LOS CIUDADANOS Y EMPRESAS, LAS INFRAESTRUCTURAS CRÍTICAS Y OPERADORES ESTRATÉGICOS, LAS REDES ACADÉMICAS Y DE INVESTIGACIÓN, ASÍ COMO LAS REDES DE DEFENSA, TIENEN A SU DISPOSICIÓN UNA SERIE DE **CSIRT** DE REFERENCIA:

- **CCN-CERT**
- **INCIBE-CERT**
- **CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD (CNPIC)**
- **ESP-DEF-CERT DEL MANDO CONJUNTO DEL CIBERESPACIO**

5. NATURALEZA Y FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES TIPO CERT NACIONALES E INTERNACIONALES

ORGANISMOS CERT/CSIRT

CCN-CERT

CON UN **ÁMBITO COMPETENCIAL EN EL SECTOR PÚBLICO GENERAL**, AUTONÓMICO Y LOCAL, Y SISTEMAS QUE MANEJAN INFORMACIÓN CLASIFICADA.

INCIBE-CERT

CON UN **ÁMBITO COMPETENCIAL EN LA CIUDADANÍA**, EL SECTOR PRIVADO Y LAS INSTITUCIONES AFILIADAS A RED IRIS (RED ACADÉMICA ESPAÑOLA), EN COORDINACIÓN CON EL CCN-CERT EN LO QUE SE REFIERE A ORGANISMOS PÚBLICOS.

5. NATURALEZA Y FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES TIPO CERT NACIONALES E INTERNACIONALES

ORGANISMOS CERT/CSIRT

CENTRO NACIONAL DE PROTECCIÓN DE INFRAESTRUCTURAS Y CIBERSEGURIDAD (CNPIC)

CON UN **ÁMBITO COMPETENCIAL EN LAS INFRAESTRUCTURAS CRÍTICAS**, OPERADORES CRÍTICOS Y SERVICIOS ESENCIALES.

ESP-DEF-CERT DEL MANDO CONJUNTO DEL CIBERESPACIO,

CON ÁMBITO **COMPETENCIAL EN LAS REDES Y LOS SISTEMAS DE** INFORMACIÓN Y TELECOMUNICACIONES DE **LAS FUERZAS ARMADAS**, ASÍ COMO AQUELLAS OTRAS REDES Y SISTEMAS QUE ESPECÍFICAMENTE SE LE ENCOMIENDEN Y QUE AFECTEN A LA DEFENSA NACIONAL.

5. NATURALEZA Y FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES TIPO CERT NACIONALES E INTERNACIONALES

ORGANISMOS CERT/CSIRT

ALGUNAS COMUNIDADES AUTÓNOMAS CUENTAN CON SU PROPIO CERT DE REFERENCIA COMO ES EL CASO DEL **CSIRT-CV EN LA COMUNITAT VALENCIANA**, **LA AGENCIA DE CIBERSEGURIDAD DE CATALUÑA, ANDALUCÍA-CERT, EL BASQUE CYBERSECURITY CENTRE, CSIRT.GAL,** ETC.

LA MAYORÍA DE LOS SERVICIOS QUE PRESTAN ESTOS CERT SON **PARA EL SECTOR PÚBLICO** (ADMINISTRACIÓN AUTONÓMICA O ENTIDADES LOCALES) O CIUDADANOS (PRINCIPALMENTE EN MATERIA DE ASESORÍA Y CONCIENCIACIÓN EN CIBERSEGURIDAD).

AndalucíaCERT CENTRO DE SEGURIDAD TIC

BASQUE CYBERSECURITY CENTRE

CSIRT-CV Centre Seguretat TIC de la Comunitat Valenciana

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

CSIRT.gal Centro de resposta a incidentes de seguridade da información

5. NATURALEZA Y FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES TIPO CERT NACIONALES E INTERNACIONALES

OTROS ORGANISMOS DE GESTIÓN DE INCIDENTES

VEAMOS LOS ORGANISMOS DE GESTIÓN DE INCIDENTES MÁS RELEVANTES A NIVEL INTERNACIONAL:

- **CERT/CC (COMPUTER EMERGENCY RESPONSE TEAM/COORDINATION CENTER)**
- **AGENCIA DE LA UNIÓN EUROPEA PARA LA CIBERSEGURIDAD (ENISA)**
- **FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS (FIRST)**

5. NATURALEZA Y FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES TIPO CERT NACIONALES E INTERNACIONALES

OTROS ORGANISMOS DE GESTIÓN DE INCIDENTES

CERT/CC (COMPUTER EMERGENCY RESPONSE TEAM/COORDINATION CENTER)

EL **CERT/CC** FUE EL PRIMER EQUIPO DE RESPUESTA Y EL MÁS CONOCIDO.

SU CREACIÓN SE PRODUJO EN 1988 POR LA AGENCIA DARPA DE EE.UU CON LA FINALIDAD DE GESTIONAR AQUELLOS INCIDENTES DE SEGURIDAD RELACIONADOS CON LOS SERVICIOS DE INTERNET.

5. NATURALEZA Y FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES TIPO CERT NACIONALES E INTERNACIONALES

OTROS ORGANISMOS DE GESTIÓN DE INCIDENTES

AGENCIA DE LA UNIÓN EUROPEA PARA LA CIBERSEGURIDAD (ENISA)

SE CREÓ POR DECISIÓN DEL CONSEJO Y PARLAMENTO EUROPEO PARA ELEVAR LOS NIVELES DE SEGURIDAD DE LAS REDES Y DEL TRATAMIENTO DE LA INFORMACIÓN DENTRO DE LA UNIÓN EUROPEA.

SE CREÓ EN 2.005 Y FIJÓ SU SEDE EN GRECIA, EN LA ISLA DE CRETA.

5. NATURALEZA Y FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES TIPO CERT NACIONALES E INTERNACIONALES

OTROS ORGANISMOS DE GESTIÓN DE INCIDENTES

FORUM OF INCIDENT RESPONSE AND SECURITY TEAMS (FIRST)

SE CREÓ EN 1.990 CON LA FINALIDAD DE AGILIZAR LOS PROCESOS DE INTERCAMBIO DE INFORMACIÓN SOBRE LOS INCIDENTES DE LOS CENTROS DE RESPUESTA A INCIDENTES DE SEGURIDAD QUE INTEGRAN LA ORGANIZACIÓN.

SE CONSIDERA LA ASOCIACIÓN GLOBAL DE LOS **CSIRT/CERT**.

CONTENIDOS

1. INTRODUCCIÓN
2. PROCEDIMIENTO DE RECOLECCIÓN DE INFORMACIÓN RELACIONADA CON INCIDENTES DE SEGURIDAD
3. EXPOSICIÓN DE LAS DISTINTAS TÉCNICAS Y HERRAMIENTAS UTILIZADAS PARA EL ANÁLISIS Y CORRELACIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD
4. PROCESO DE VERIFICACIÓN DE LA INTRUSIÓN
5. NATURALEZA Y FUNCIONES DE LOS ORGANISMOS DE GESTIÓN DE INCIDENTES TIPO CERT NACIONALES E INTERNACIONALES

RESUMEN

LA **GESTIÓN DE INCIDENTES** ES LA PARTE DE LA SEGURIDAD QUE SE ENCARGA DE ASIGNAR LOS RECURSOS A LA PREVENCIÓN, DETECCIÓN Y CORRECCIÓN DE INCIDENTES QUE AFECTEN A LA SEGURIDAD DE LA INFORMACIÓN.

ESTA GESTIÓN CONLLEVA UNA SERIE DE PASOS A SEGUIR:

PREPARACIÓN Y PREVENCIÓN, DETECCIÓN Y NOTIFICACIÓN, ANÁLISIS PRELIMINAR, CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN, INVESTIGACIÓN Y ACTIVIDADES POSTERIORES.

RESUMEN

TODOS ESTOS PASOS AYUDAN A LAS ORGANIZACIONES A OBTENER MÁS INFORMACIÓN DEL INCIDENTE, EVALUAR LOS DAÑOS CAUSADOS, TOMAR MEDIDAS AL RESPECTO Y A CONSEGUIR LLEGAR AL PUNTO INICIAL EN EL MENOR TIEMPO POSIBLE.

ADEMÁS, CON LA RECOLECCIÓN DE INFORMACIÓN SE CONSIGUE ANALIZAR TODO EL PROCEDIMIENTO LLEVADO A CABO POR EL INCIDENTE Y ELABORAR MEDIDAS PREVENTIVAS EVITANDO QUE ESTE INCIDENTE SE VUELVA A PRODUCIR.

RESUMEN

POR SU PARTE, **LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN BASADA EN EL ANÁLISIS Y CORRELACIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (CON HERRAMIENTAS SIM, SEM Y SIEM)** FACILITARÁ AL RESPONSABLE DE SEGURIDAD EL CONOCIMIENTO DE TODO LO QUE SUCEDE EN LOS EQUIPOS A TIEMPO REAL Y ASÍ, CONSEGUIR ESTABLECER MEDIDAS DE CONTENCIÓN MÁS EFECTIVAS Y RÁPIDAS EN CUANTO SE DETECTE ALGÚN INDICIO DE INCIDENTE DE SEGURIDAD.

RESUMEN

UNA VEZ DETECTADO Y ELIMINADO EL INCIDENTE Y RESTAURADA LA SITUACIÓN ORIGINAL DEBE PROCEDERSE A **LA INVESTIGACIÓN Y VERIFICACIÓN DEL INCIDENTE** CON EL FIN DE ELABORAR UN **INFORME FINAL** QUE CONTENGA ASPECTOS FUNDAMENTALES ACERCA DE LAS CAUSAS Y CONSECUENCIAS PRODUCIDAS POR EL INCIDENTE, LA EVALUACIÓN DE LA TOMA DE DECISIONES Y ACTUACIONES LLEVADAS A CABO POR EL EQUIPO DE RESPUESTA A INCIDENTES, EL ANÁLISIS DE LAS POLÍTICAS DE SEGURIDAD Y EL ANÁLISIS DE LAS DIRECTRICES DE LA ORGANIZACIÓN.

RESUMEN

PARA ESTABLECER ESTAS MEDIDAS Y HERRAMIENTAS HAY UNA SERIE DE ORGANIZACIONES NACIONALES E INTERNACIONALES CONOCIDAS COMO **CERT O CENTROS DE RESPUESTA A INCIDENTES DE SEGURIDAD EN TECNOLOGÍAS** DE LA INFORMACIÓN ENCARGADAS DE DISEÑAR MEDIDAS PREVENTIVAS Y REACTIVAS, MANTENER BASES DE DATOS DE INCIDENTES ACTUALIZADAS Y, EN GENERAL, DE APOYAR Y OFRECER INFORMACIÓN VALIOSA A LAS ORGANIZACIONES QUE LES AYUDEN A ELABORAR UN PLAN DE GESTIÓN DE INCIDENTES DE MAYOR CALIDAD.

ESTO ES TODO