Perfil Profesional

UC0488_3

DETECTAR Y RESPONDER ANTE INCIDENTES DE SEGURIDAD

MF0488_3

GESTIÓN DE INCIDENTES DE SEGURIDAD INFORMÁTICA

Realizaciones profesionales y criterios de realización

* RP1: Implantar procedimientos para la respuesta ante incidentes e implantar mecanismos para la detección de intrusos según directrices de los equipos de respuesta ante incidentes nacionales e internacionales.
* RP2: Detectar incidentes de seguridad de forma activa y preventiva para minimizar el riesgo según directrices de los equipos de respuesta ante incidentes nacionales e internacionales.
* RP3: Coordinar la respuesta ante incidentes de seguridad entre las distintas áreas implicadas para contener y solucionar el incidente según los requisitos de servicio y dentro de las directivas de la organización.

RP1

* CR1.1 Los procedimientos de detección y respuesta de incidentes están documentados, indican los roles y responsabilidades de seguridad e implementan los requerimientos de la política de seguridad de la organización.
* CR1.2 Los sistemas se modelan para detectar signos de comportamiento sospechoso seleccionando los mecanismos de registro a activar, observando las alarmas definidas, caracterizando los parámetros de utilización de la red e inventariando los archivos para detectar modificaciones.
* CR1.3 Los mecanismos de registro del sistema se activan y se planifican los procedimientos de análisis de los mismos según las especificaciones de seguridad de la organización.
* CR1.4 Los sistemas de detección de intrusos se instalan, actualizan y configuran en función de las especificaciones de seguridad de la organización.
* CR1.5 Los procedimientos de restauración del sistema informático se verifican para la recuperación del mismo ante un incidente grave dentro de las necesidades de la organización.

RP2

* CR2.1 Las herramientas utilizadas para detectar intrusiones son analizadas para determinar que no han sido comprometidas ni afectadas por programas maliciosos.
* CR2.2 Los parámetros de funcionamiento sospechoso se analizan con herramientas específicas según la normativa de seguridad.
* CR2.3 Los componentes software del sistema se verifican periódicamente en lo que respecta a su integridad usando programas específicos.
* CR2.4 Las pruebas realizadas a los dispositivos de protección física del sistema informático verifican el correcto funcionamiento de los mismos según la normativa de seguridad de la organización.
* CR2.5 Los sucesos y signos extraños que pudieran considerarse una alerta son recogidos en el informe diario de actividad.

RP3

* CR3.1 La detección de un incidente de seguridad produce la realización de los procedimientos recogidos en los protocolos de la normativa de seguridad de la organización.
* CR3.2 El sistema vulnerado, se aísla y se procede a recoger la información para el análisis forense de la misma según los procedimientos de la normativa de seguridad de la organización.
* CR3.3 El sistema atacado se analiza mediante herramientas de detección de intrusos según los procedimientos de seguridad de la organización.
* CR3.4 La intrusión es contenida mediante la aplicación de las medidas establecidas en la normativa de seguridad de la organización.
* CR3.5 La documentación del incidente se realiza para su posterior análisis e implantación de medidas que impidan la replicación del hecho sobrevenido.
* CR3.6 Los daños causados se determinan y se planifican las posibles acciones para continuar la normal prestación de servicios del sistema vulnerado según las normas de calidad y el plan de explotación de la organización.

Contexto profesional
Medios de producción

* Aplicaciones ofimáticas corporativas.
* Analizadores de vulnerabilidades.
* Herramientas para garantizar la confidencialidad de la información.
* Programas que garantizan la confidencialidad e integridad de las comunicaciones.
* Aplicaciones para gestión de proyectos.
* Programas de análisis de contraseñas.
* Software de monitorización de redes.
* Software de flujo de trabajo para envío de alarmas e incidencias a responsables.
* IDS y sus consolas.
* Consola de SNMP.

Contexto profesional
Productos y resultados

* Informes de análisis de vulnerabilidades.
* Relación de contraseñas débiles.
* Registro de ficheros de datos de carácter personal, según normativa vigente.
* Informe de auditoría de servicios y puntos de acceso al sistema informático.
* Registro de actividad.
* Documento de seguridad.
* Registro de alarmas.

Contexto Profesional
Información utilizada o generada

* Normativa sobre protección de datos personales.
* Política de seguridad de la empresa.
* Metodologías de análisis de seguridad (OSSTM, BS7799/ISO17799).
* Boletines de seguridad y avisos de vulnerabilidades, en su mayoría redactados en inglés, y disponibles en formato electrónico.
* Documento de trabajo en base a la política de seguridad.
* Normativa de detección de intrusos.
* Normativa de prevención de amenazas de seguridad.