Estándar de competencias profesionales

Gestionar incidentes de ciberseguridad

Familia Profesional	**Informática y Comunicaciones**
Nivel	**3**
Código	**ECP0488_3**
Estado	**BOE**
Publicación	**RD 917/2024**

Competencia profesional

Elementos de la competencia

EC1 Implantar procedimientos para la respuesta ante incidentes y mecanismos para la detección de intrusos en los sistemas de una entidad u organización según directrices ante incidentes nacionales e internacionales para los equipos de respuesta.

IC1.1 Los procedimientos de detección y respuesta de incidentes se localizan, verificando que están documentados, que indican los roles y responsabilidades de seguridad y que implementan los requerimientos de la política de seguridad de la entidad, así como la determinación de la cadena de mando ante la detección de un incidente de seguridad.

IC1.2 La modelización de los sistemas se efectúa, seleccionando los mecanismos de registro a activar, observando las alertas definidas, caracterizando los parámetros de utilización de la red e inventariando los archivos para detectar modificaciones y signos de comportamiento sospechoso a partir de indicadores de compromiso (IOC: "Indicator of Compromise") facilitados por equipos de respuesta ante incidentes nacionales e internacionales.

IC1.3 La activación de los mecanismos de registro del sistema se verifica, contrastándolos con las especificaciones de seguridad de la organización y/o mediante un sistema de indicadores y métricas.

IC1.4 La planificación de los mecanismos de análisis de registros se verifica, de forma que se garantice la detección de los comportamientos sospechosos, mediante un sistema de indicadores y métricas.

IC1.5 La instalación, configuración y actualización de los sistemas de detección de intrusos (IDS) se verifica en función de las especificaciones de seguridad de la organización y/o mediante un sistema de indicadores y métricas.

IC1.6 Los procedimientos de restauración del sistema informático, establecidos en el Plan de recuperación ante desastres (DRP: "Disaster Recovery Plan") definido por la organización, se verifican, comprobando que pueden ser recuperados en tiempo y forma ante un incidente grave.

EC2 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 y de la entidad responsable del sistema.

IC2.1 Las herramientas utilizadas para detectar intrusiones se comprueba que no han sido comprometidas ni afectadas por programas maliciosos analizándolas, siguiendo las guías y directrices de los equipos de respuesta nacionales e internacionales.

IC2.2 Los funcionamientos sospechosos se detectan, analizando parámetros de funcionamiento tales como conexiones no autorizadas, mensajes de alerta de los sistemas de detección de intrusiones (IDS: "Intrusion Detection System") o "antimalware" entre otros, usando herramientas específicas tales como sistemas de Gestión de información y eventos de seguridad (SIEM: "Security information and event management") e IDS, entre otras y estableciendo procedimientos para recoger denuncias de los usuarios acerca de ataques tales como "phising" o comportamientos anómalos en equipos según directrices de la entidad responsable del sistema.

IC2.3 Los componentes "software" del sistema se verifican periódicamente en lo que respecta a su integridad usando programas específicos.

IC2.4 El funcionamiento de los dispositivos de protección física se verifica por medio de los registros de cada sistema, pruebas específicas, pruebas de estrés, entre otras según las normas de la organización y/o normativa aplicable de seguridad.

IC2.5 Los sucesos y signos extraños que pudieran considerarse una alerta se recogen en el informe para su posterior análisis, en función de la gravedad de los mismos y la política de la organización, especificando para cada uno ítems tales como día y hora de la detección, persona que lo comunicó, sistemas implicados y acciones realizadas, entre otros.

IC2.6 La exposición o filtración de los datos de la organización se verifica periódicamente en función del riesgo que haya determinado la entidad responsable del sistema, consultando fuentes abiertas (OSINT: "Open Source Intelligence") según las características de la organización.

IC2.7 La información publicada por los centros de respuesta ante incidentes nacionales y/o internacionales se comprueba, verificándola de manera periódica para establecer en su caso

los mecanismos de seguridad recomendados en caso de exposición a las amenazas publicadas.

EC3 Coordinar la respuesta ante incidentes de seguridad entre las áreas implicadas, aplicando el procedimiento recogido en los protocolos de seguridad para contener y solucionar el incidente según los requisitos de servicio y dentro de las directivas de la entidad u organización a proteger.

IC3.1 Los procedimientos se activan ante la detección de un incidente de seguridad, dando aviso a los responsables de cada subsistema y aplicando los pasos recogidos en los protocolos de la normativa de seguridad de la organización.

IC3.2 La información para el análisis forense del sistema vulnerado se recoge, una vez aislado el sistema, capturando una imagen tan precisa como sea posible, realizando notas detalladas (incluyendo fechas y horas indicando si se utiliza horario local o UTC), recogiendo la información según el orden de volatilidad (de mayor a menor) entre otras, según los procedimientos de las normas de seguridad de la entidad.

IC3.3 Las características de la intrusión se determinan, analizando el sistema atacado mediante herramientas de detección de intrusos (IDS), usando las facilidades específicas de cada herramienta y según los procedimientos de seguridad de la organización.

IC3.4 La intrusión se contiene mediante la aplicación de las medidas establecidas en las normas de seguridad de la organización tales como desconexión de equipos y/o segmentos de red o cierre de puertos de comunicaciones, entre otras, y aquellas extraordinarias, que indique la persona responsable de la seguridad, aunque no estén previamente planificadas.

IC3.5 La documentación del incidente, así como todas las acciones realizadas y las conclusiones obtenidas se realiza para su posterior análisis e implantación de medidas que impidan la replicación del hecho sobrevenido, manteniendo de esta forma un registro de lecciones aprendidas ("Lessons Learned").

IC3.6 Las posibles acciones para continuar la normal prestación de servicios del sistema vulnerado se planifican a partir de la determinación de los daños causados, cumpliendo los criterios de calidad de servicio y el plan de explotación de la entidad a proteger.

EC4 Implantar planes de prevención y concienciación en ciberseguridad, para facilitar la previsión de ciberincidentes y su respuesta, en caso de producirse, según los requisitos de servicio y dentro de las directivas de la organización o entidad a proteger.

IC4.1 Las medidas de ciberseguridad definidas por la organización se difunden, usando medios tales como correo electrónico, intranet corporativa y sesiones específicas, entre otros.

IC4.2 La normativa de protección del puesto de trabajo se establece, incluyendo ítems tales como escenarios y ejemplos de riesgo y medidas de seguridad, entre otros.

IC4.3 El plan de concienciación de ciberseguridad dirigido a los empleados se define, elaborando material y cursos o tutoriales para su difusión o impartición y las evaluaciones a realizar y su periodicidad.

IC4.4 El material y cursos necesarios para llevar a cabo las acciones de concienciación dirigidas a los empleados se difunde o en su caso se imparte de forma periódica, usando los mecanismos disponibles en la entidad, tales como correo electrónico, plataformas web de difusión, aulas y canales de vídeo para cursos, entre otros, capacitando a los empleados ante ciberataques, para detectar los métodos y vectores más habituales.

Contexto profesional

Ámbito profesional

Sectores productivos

Ocupaciones y puestos de trabajo relevantes

Medios de producción

Equipos informáticos tales como ordenadores de sobremesa, portátiles y servidores. Aplicaciones ofimáticas corporativas. Analizadores de vulnerabilidades tales como antivirus/"antimalware" o EPP ("Endpoint Protection Platform") y EDR ("Endpoint Detection" and "Response"). Herramientas para garantizar la confidencialidad de la información tales como sistemas de detección de intrusiones (IDS), sistemas de prevención de intrusiones (IPS). "Software" de monitorización de redes. Sistemas de monitorización SIEM ("Security Information and Event Management"). "Software" para garantizar la confidencialidad e integridad de las comunicaciones. Programas de análisis de contraseñas. "Software" de flujo de trabajo para envío de alarmas e incidencias a responsables. Consola de SNMP. Herramientas de análisis forense (creación de líneas de tiempo, recuperación de ficheros borrados, clonado de discos, entre otros).

Información utilizada o generada

Normas externas de trabajo (normativa aplicable de propiedad intelectual e industrial; normativa aplicable de protección de datos y seguridad informática; normativa aplicable sobre prevención de riesgos laborales -ergonomía-). Normas internas de trabajo (plan de seguridad, metodologías de análisis de seguridad, histórico de incidencias, registro de ficheros de datos de carácter personal, informes de análisis

de vulnerabilidades, relación de contraseñas débiles, informe de auditoría de servicios y puntos de acceso al sistema informático, normas internas de detección de intrusos y de prevención de amenazas de seguridad). Documentación técnica (boletines de seguridad externos y avisos de vulnerabilidades, documentación técnica del fabricante de los equipos, sistemas y "software" utilizado, documentación técnica de la red, bibliografía especializada, tutoriales y cursos).