Estándar de competencias profesionales

Responder ante eventos de ciberseguridad

Familia Profesional	**Informática y Comunicaciones**
Nivel	**2**
Código	**ECP2798_2**
Estado	**BOE**
Publicación	**RD 917/2024**

Competencia profesional

Elementos de la competencia

EC1 Implementar eventos y alertas de seguridad, configurando los parámetros relacionados, siguiendo especificaciones recibidas de la persona responsable de la administración de los sistemas, para garantizar su seguridad, según normas y procedimientos de la entidad responsable.

IC1.1 Los eventos de sistemas recolectados en el sistema de monitorización se parametrizan configurándolos de modo que se asegure que la información que proporciona es completa y precisa para facilitar su posterior tratamiento.

IC1.2 Las reglas de tratamiento de los eventos normalizados se implementan, configurándolas en función de su severidad para la generación de alertas.

IC1.3 Las reglas de correlación entre eventos normalizados y alertas se implementan, configurándolas en función de su severidad para la generación de alertas.

IC1.4 Las reglas de agregación de eventos normalizados y alertas se implementan, configurando métricas y elementos para su agrupación.

IC1.5 Los mecanismos de remediación automática o semiautomática de las alertas son implementados, de acuerdo con las condiciones de remediación.

IC1.6 La documentación de las alertas y reglas de normalización, agregación y correlación realizados se confecciona, siguiendo los modelos internos establecidos por la organización,

recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

EC2 Ejecutar procedimientos frente alertas de seguridad, identificando parámetros, origen y condiciones y comunicando a las personas responsables de su gestión, para subsanar incidencias de seguridad, según normas y procedimientos de la entidad responsable.

IC2.1 El procedimiento operativo de seguridad a aplicar ante las alertas generadas por el sistema de monitorización se selecciona, interpretando cada alerta y consultando el maestro de alertas y procedimientos establecido por la organización.

IC2.2 Los procedimientos de seguridad se aplican, de acuerdo con las condiciones de entorno de la alerta específica, identificando parámetros relacionados tales como direcciones IP origen y destino, puerto accedido, tipo de evento, entre otros.

IC2.3 El escalado de alertas se ejecuta, comunicándolas a la persona o personas responsables de su gestión, junto con información tal como resultado del evento, IP origen y destino y puertos, entre otros datos.

IC2.4 Las alertas gestionadas se cierran, indicando si se trata de una alerta real o un falso positivo, el mecanismo de resolución y grado de afectación.

IC2.5 La documentación relativa a las alertas gestionadas se confecciona, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

EC3 Colaborar en la definición de procedimientos de respuesta a alertas de seguridad, recabando requisitos, condiciones de entorno y objetivos, definiéndolos y registrándolos, para preparar la respuesta ante incidencias, según normas y procedimientos de la entidad responsable.

IC3.1 Las alertas sin procedimiento asociado se marcan en la documentación para su uso posterior, utilizando el maestro de alertas y procedimientos operativos e identificando aquellas alertas no recogidas en él.

IC3.2 Los requisitos, condiciones de entorno y objetivos de remediación para cada alerta se recaban, previa identificación, documentándolos según modelos internos establecidos por la organización, para su control, uso y trazabilidad.

IC3.3 Los procedimientos de seguridad, considerando la alerta, las condiciones de entorno, los objetivos de remediación y los requisitos de remediación decididos por la persona responsable, se redactan, indicando las acciones a realizar y prestando especial atención a los requisitos de continuidad de negocio definidas por la organización.

IC3.4 Los procedimientos de seguridad se prueban, verificando su aplicación y aprobándolos y registrándolos de acuerdo con el modelo definido por la organización.

IC3.5 La documentación de los procesos realizados se confecciona, siguiendo los modelos internos establecidos por la organización, recogiendo las configuraciones y/o acciones aplicadas y archivándola para su control, trazabilidad y uso posterior.

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. Conexión a red. Navegadores. Buscadores. Servidores y clientes de redes privadas virtuales (VPN). Programas de conexión segura a servicios telemáticos. Analizadores de vulnerabilidades. Antivirus/"antimalware". EPP ("Endpoint Protection Platform"). EDR ("Endpoint Detection" and "Response"). 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") y de recolección de información (tipo "Syslog"). "Software" para garantizar la confidencialidad e integridad de las comunicaciones. Consola de SNMP. "Software" de flujo de trabajo para envío de alarmas e incidencias a responsables.

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, procedimientos y políticas de seguridad, histórico de ataques e incidencias, informes de análisis de vulnerabilidades, relación de contraseñas débiles, informe 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).