

TABLA 3: Identificación de las partes de las Competencias

| CPPS | Qué | Cómo | Para Qué |
|------|---|--|----------|
| a) | Elaborar e implementar planes de prevención y concienciación en ciberseguridad en la organización | aplicando la normativa vigente | |
| b) | Detectar e investigar incidentes de ciberseguridad | documentándolos e incluyéndolos en los planes de securización de la organización | |
| k) | Elaborar documentación técnica y administrativa cumpliendo con la legislación vigente | respondiendo a los requisitos establecidos | |
| 1) | Adaptarse a las nuevas situaciones laborales | manteniendo actualizados los conocimientos científicos, técnicos y tecnológicos relativos a su entorno profesional, gestionando su formación y los recursos existentes en el aprendizaje a lo largo de la vida | |



| m) | Resolver situaciones, problemas o contingencias con iniciativa y autonomía en el ámbito de su competencia | con creatividad, innovación y espíritu de mejora en el trabajo personal y en el de los miembros del equipo | |
|----|---|---|--|
| n) | Generar entornos seguros en el desarrollo de su trabajo y el de su equipo | supervisando y aplicando los procedimientos de prevención de riesgos laborales y ambientales, de acuerdo con lo establecido por la normativa y los objetivos de la organización | |
| ñ) | Supervisar y aplicar procedimientos de gestión de calidad, de accesibilidad universal y de «diseño para todas las personas», en las actividades profesionales incluidas en los procesos de producción o prestación de servicios | | |



TABLA 4: Identificación de las partes de los Objetivos

| OG | Qué | Cómo | Para Qué |
|----|---|---|--|
| a) | Identificar los principios de la organización y normativa de protección en ciberseguridad | planificando las acciones que es preciso adoptar en el puesto de trabajo | para la elaboración del plan de prevención y concienciación |
| b) | Auditar el cumplimiento del plan de prevención y concienciación de la organización | definiendo las acciones correctoras que puedan derivarse | para incluirlas en el plan se securización de la organización |
| c) | Detectar incidentes de ciberseguridad | implantando los controles, las herramientas y los mecanismos necesarios | para su monitorización e identificación |
| d) | Analizar y dar respuesta a incidentes de ciberseguridad, | identificando y aplicando las medidas necesarias | para su mitigación, eliminación, contención o recuperación |
| q) | Desarrollar manuales de información | utilizando herramientas ofimáticas y de diseño asistido por ordenador | para elaborar documentación técnica y administrativa |



| r) | Analizar y utilizar los recursos y oportunidades de aprendizaje relacionados con la evolución científica, tecnológica y organizativa del sector y las tecnologías de la información y la comunicación | | para mantener el espíritu de actualización y adaptarse a nuevas situaciones laborales y personales |
|----|---|---|--|
| s) | Desarrollar la creatividad y el espíritu de innovación | | para responder a los retos que se presentan en los procesos y en la organización del trabajo y de la vida personal |
| t) | Evaluar situaciones de prevención de riesgos laborales y de protección ambiental | proponiendo y aplicando medidas de prevención personales y colectivas, de acuerdo con la normativa aplicable en los procesos de trabajo | para garantizar entornos seguros |
| u) | Identificar y proponer las acciones profesionales necesarias | | para dar respuesta a la accesibilidad universal y al «diseño para todas las personas» |



| | | para valorar la |
|----|---|--------------------|
| | Idontificar y anlicar | cultura de la |
| | Identificar y aplicar parámetros de calidad | evaluación y de la |
| | en los trabajos y | calidad y ser |
| v) | actividades realizados | capaces de |
| | | supervisar y |
| | en el proceso de | mejorar |
| | aprendizaje | procedimientos de |
| | | calidad |

TABLA 5: Asociación de Competencias y Objetivos

| OG | CPPS |
|----|------|
| a) | a) |
| b) | b) |
| c) | b) |
| d) | b) |
| q) | k) |
| r) | l) |
| s) | m) |
| t) | n) |
| u) | ñ) |
| v) | ñ) |



TABLA 6: ANEXO A OG

| OG | Qué | Cómo | Para Qué | RA |
|----|---|--|---|--|
| a) | Identificar los principios de la organización y normativa de protección en ciberseguridad | planificando las acciones que es preciso adoptar en el puesto de trabajo | para la elaboración del plan de prevención y concienciación | 1. Desarrolla planes de prevención y concienciación en ciberseguridad, estableciendo normas y medidas de protección. |
| b) | Auditar el cumplimiento del plan de prevención y concienciación de la organización | definiendo las acciones correctoras que puedan derivarse | para incluirlas en el plan se securización de la organización | 1. Desarrolla planes de prevención y concienciación en ciberseguridad, estableciendo normas y medidas de protección. |
| c) | Detectar incidentes de ciberseguridad | implantando los controles, las herramientas y los mecanismos necesarios | para su monitorización e identificación | 2. Analiza incidentes de ciberseguridad utilizando herramientas, mecanismos de |



| d) | Analizar y dar respuesta a incidentes de ciberseguridad, | identificando y aplicando las medidas necesarias | para su mitigación, eliminación, contención o recuperación | detección y alertas de seguridad. 3. Investiga incidentes de ciberseguridad analizando los riesgos implicados y definiendo las posibles medidas a adoptar. 5. Detecta y |
|----|---|---|--|---|
| q) | Desarrollar manuales de información | utilizando herramientas ofimáticas y de diseño asistido por ordenador | para elaborar documentación técnica y administrativa | documenta incidentes de ciberseguridad siguiendo procedimientos de actuación establecidos. |
| r) | Analizar y utilizar los recursos y oportunidades de aprendizaje relacionados con la evolución científica, | manteniendo actualizados los conocimientos científicos, técnicos y tecnológicos relativos a su entorno profesional, | para mantener el espíritu de actualización y adaptarse a nuevas situaciones laborales y personales | 3. Investiga incidentes de ciberseguridad analizando los riesgos implicados y definiendo |



| | tecnológica y | gestionando su | | las posibles |
|----|------------------|------------------|-----------------|----------------|
| | organizativa del | formación y los | | medidas a |
| | sector y las | recursos | | adoptar. |
| | tecnologías de | existentes en el | | |
| | la información | aprendizaje a lo | | |
| | y la | largo de la vida | | |
| | comunicación | | | |
| | | | | 4. Implementa |
| | | | | medidas de |
| | | con creatividad, | para responder | ciberseguridad |
| | | innovación y | a los retos que | en redes y |
| | Desarrollar la | espíritu de | se presentan | sistemas |
| | creatividad y el | mejora en el | en los | respondiendo a |
| s) | espíritu de | trabajo | procesos y en | los |
| | innovación | personal y en el | la organización | incidentes |
| | IIIIOVacion | de los miembros | del trabajo y | detectados y |
| | | del equipo | de la vida | aplicando las |
| | | | personal | técnicas de |
| | | | | protección |
| | | | | adecuadas. |
| | | proponiendo y | | 4. Implementa |
| | | aplicando | | medidas de |
| | Evaluar | medidas de | | ciberseguridad |
| | situaciones de | prevención | | en redes y |
| | prevención de | personales y | para garantizar | sistemas |
| t) | riesgos | colectivas, de | entornos | respondiendo a |
| | laborales y de | acuerdo con la | seguros | los |
| | protección | normativa | | incidentes |
| | ambiental | aplicable en los | | detectados y |
| | | procesos de | | aplicando las |
| | | trabajo | | técnicas de |



| | | | | protección |
|----|--------------------|-----------------|-------------------------------------|----------------|
| | | | | adecuadas. |
| | | Supervisando y | | |
| | | aplicando | | |
| | | procedimientos | | 4. Implementa |
| | | de gestión de | | medidas de |
| | | calidad, de | | ciberseguridad |
| | | accesibilidad | para dar | en redes y |
| | Identificar y | universal y de | respuesta a | sistemas |
| | proponer las | «diseño para | la accesibilidad | respondiendo a |
| u) | acciones | todas las | universal y al | los |
| | profesionales | personas», en | «diseño para | incidentes |
| | necesarias | las actividades | todas las | detectados y |
| | | profesionales | personas» | aplicando las |
| | | incluidas | | técnicas de |
| | | en los procesos | | protección |
| | | de producción o | | adecuadas. |
| | | prestación de | | |
| | | servicios | | |
| | | Supervisando y | para valorar la | |
| | Identificar y | aplicando | cultura de la | 5. Detecta y |
| | aplicar | procedimientos | evaluación y | documenta |
| | parámetros de | de gestión de | de la calidad y | incidentes de |
| | calidad en los | calidad, de | ser | ciberseguridad |
| v) | trabajos y | accesibilidad | capaces de | siguiendo |
| | actividades | universal y de | supervisar y mejorar procedimientos | procedimientos |
| | realizados | «diseño para | | de |
| | en el proceso de | todas las | | actuación |
| | 0.1 0. p. 00000 ao | | | |
| | aprendizaje | personas», en | de calidad | establecidos. |



| Alisel (| | |
|----------|-----------------|--|
| | profesionales | |
| | incluidas | |
| | en los procesos | |
| | de producción o | |
| | prestación de | |
| | servicios | |