

BASES ESPECIFIQUES

Codi del procés selectiu: ATL027-22TRE

1- Dades de la plaça

Lloc de treball: Responsable de Seguretat de la Informació
Número de places convocades: 1
Classe de personal: laboral fix
Grup professional: 10
Centre de treball d'adscripció: OC Font Santa
Adreça: C/Sant Martí de l'Erm, 30. Sant Joan Despí (Barcelona)
Jornada: completa
Règim horari: Horari general d'empresa
Sistema de selecció: Concurs oposició

2- Funcions del lloc:

Les principals funcions a desenvolupar assignades al lloc de treball seran:

Les principals funcions a desenvolupar assignades al lloc de treball seran:

- Participar en l'establiment dels criteris pel desenvolupament de la planificació estratègica i objectius de l'oficina del CISO.
- Impulsar el desenvolupament i manteniment del "Sistema de gestió de Seguretat de la Informació" (SGSI).
- Impulsar el desenvolupament i implantació d'un marc de gestió del risc
- Analitzar i prevenir els riscos dels sistemes d'informació de forma periòdica.
- Participar en la definició, manteniment i desplegament del pla de continuïtat de negoci.
- Coordinar la definició de l'arquitectura de ciberseguretat
- Proposar i gestionar eines apropiades pel correcte manteniment de la seguretat
- Definir i gestionar els informes periòdics dels diferents dominis de seguretat.
- Definir i mantenir les mesures de monitorització de la seguretat.
- Gestionar projectes de ciberseguretat.
- Coordinar el desplegament del Pla director de ciberseguretat
- Impulsar la formació i divulgació en matèria de seguretat entre el personal de l'empresa.
- Realitzar el seguiment de la normativa i legislació vigent per tal de verificar la correcta aplicació.
- Coordinar l'auditoria periòdica per garantir compliment dels requeriments de seguretat establerts al pla de seguretat.
- Fer seguiment del mercat tecnològic i de proveïdors d'interès relacionats amb matèria de ciberseguretat.

3- Requeriments específics

3.1. Titulació exigida

- Titulació grau mig o superior en informàtica, telecomunicacions o altra carrera tècnica assimilable amb experiència demostrada.
- 2 - 3 anys experiència contrastada en projectes vinculats a l'entorn de seguretat de la informació.
- Disposar del coneixement oral i escrit de la llengua catalana de nivell de suficiència de català C1 de la Direcció General de Política Lingüística, o l'equivalent.
- Carnet de conduir B i capacitat per desplaçar-se habitualment.

3.2. Competències requerides

- Postgrau o màster Universitari en gestió de la ciberseguretat.
- Coneixements relatius als dominis de seguretat (ISO/IEC 27001 y 27002, ISO 38500 COBIT, NIS, etc.): Govern de la ciberseguretat, Seguretat d'informació i gestió de riscos, Protecció d'actius tecnològics i d'informació, Seguretat de xarxes, Gestió d'identitat i control d'accés, Continuitat de negoci i plans de recuperació, Legislació i compliment normatiu (RGPD, NIS, PIC, etc.), Seguretat d'operacions i Seguretat d'aplicacions.
- Coneixements bàsics de sistemes de control: Capacitat d'interlocució i conèixer els aspectes mínims dels sistemes de control (SCADAS, PLC, SIC, etc.)
- Coneixements de xarxes a nivell de CCNA o CCNP: Elements de seguretat perimetral - FW, radius, control d'accessos, IPS/IDS,, segmentacions (VLAN, routing, etc.), creació de DMZs, etc.
- Coneixements d'entorns virtuals, SO i BBDD: VMWare, Hyper-V, KVM, Windows, Linux, SQL, etc.
- Disposar del coneixement oral i escrit de la llengua anglesa. Nivell acreditat mínim B2 escola oficial d'idiomes.

4- Temari específic

Tema 1. Xarxes IT/OT. Estàndards comunicacions. Model OSI. Protocols. Arquitectures segures IT/OT.

Tema 2. Hacking Ètic. Information gathering. Escaneig i enumeració. Vulnerabilitats comuns. Anàlisi automatitzat. Explotació i gestió vulnerabilitats.

Tema 3. Monitorització Events de Seguretat. Registres propis del sistema. Sistemes de detecció i monitorització. Fonts heterogènies de dades. Correlació de logs.

Tema 4. Cloud Security y Edge Computing. Tipus de cloud. Seguretat al cloud. Seguretat principals plataformes (AWS, Azure, Goolge). Containers.

Tema 5. IoT. Visió general. Arquitectures segures. Protocols.

Tema 6. Data Driven Security. Data science. Anàlisi de dades amb R y Python.

Tema 7. Resposta a Incidents. Visió general. Eines d'atac. Logs crítics. Anàlisi forense.

Tema 8. Anàlisi de Malware. Visió general. Anàlisi estàtic. Anàlisi dinàmic. Anàlisi de memòria. Reversing.

Tema 9. Blockchain i Autenticació. Criptografia simètrica o de clau secreta. Criptografia asimètrica o de clau pública. Infraestructura de clave pública (PKI). Protocols de seguretat. Distributed Ledger Technolgy - Blockchain. Serveis de confiança i identitat digital. Federació d'identitats

Tema 10. Secure Software Development Life Cycle (SSDLIC). Metodologia SSDLC. Principis de seguretat i requeriments de disseny. Definició i planificació del programa de proves. Automatització de proves d'integració i pas a producció CI/CD.

Tema 11. Disseny, Desenvolupament i Implantació. Arquitectura de seguretat. Disseny de controls físics i lògics. Gestió de roles. Controls específics cloud. Arquitectura Zero Trust

Tema 12. Anàlisi de Riscos i Ciberresiliència. Ciberresiliència. Estàndards de seguretat i privadesa de la informació. Anàlisi i gestió de riscos i les seves metodologies. Organització de la seguretat de la informació. Continuïtat de negoci.

Tema 13. Compliment. Marc compliment. Política seguretat i normes. Sistemes de gestió. Privadesa i Reglament General de Protecció de Dades (RGPD). Esquema Nacional de Seguretat. NIS 2.

Tema 14. Govern de la ciberseguretat. Marcs i model de govern de la ciberseguretat. Gestió estratègica de la ciberseguretat. Eines de govern. Optimització de recursos eines de reporting. Model de govern del cloud.

Tema 15. Auditoria de Sistemes de Informació. Procés d'auditoria als sistemes d'informació. Govern i gestió de TI. Adquisició, desenvolupament i implementació de sistemes d'informació. Operacions dels sistemes d'informació i resiliència del negoci. Protecció dels actius d'informació.

Tema 16. La prevenció de riscos laborals: obligacions dels treballadors en matèria de prevenció de riscos. Seguretat i salut laboral: definició de risc laboral, definició d'accident laboral i les seves tipologies. Definició i utilitat dels equips de protecció individual. Plans d'Autoprotecció (PAU). Prevenció i classificació de les emergències, Mètode PAS. Primers auxilis. Evacuació i punt de trobada.