* Identificar y documentar actividades ile.  gules o fraudulentas en la empresa  Rewpilar y preservar pruebas concretas pan  su uso en el proceso  Sistemas Operativos  - Redes  Areas que evalva - Almacenamiento de datos	Tipo de auditoria: Auditorio de seguridad de redes  Obsetivo:  Tidentificar vulnerabilidades evatuar politicas de seguridad verificar el complimiento de normativas, prevenir acceso no autoritado  Areas que evalva e Protección de clatos e Configuraciones de la red Monitoreo y respuesta a incidentes  Tipo de auditoria Auditoria a controles de acceso a sistemas  Obsectivo e Evalvar la efectividad de las medidas de seguridad implementadas para proteger la información y recursos de una erganificación  Areas que evalva e Autenticación y autoricación so Políticas de control de acceso y peníos de Registro y monitores de acceso y peníos de Registro y monitores de acceso y peníos y peníos de acceso y peníos y peníos de acceso y peníos y peníos de acceso y peníos y peníos y peníos de acceso y peníos y pen	Nous Laborer	
Obsetivo:  VIdentificar vulnerabilidades evalvar politicas de segundad verificar el complimiento de normalivas i pievenir uccesos no polonizado  Areas que evalva Control de acceso en Protección de datas Configuraciones de la red Monitoreo y respuesta a inicidentes  Tipo de auditoria Auditoria a controles de acceso a sistemas  Obsectivo Evalvar la efectividad de las medidas de segundad implementadas para proteger la información y recursos de una organización  12 Gestión de usuaras y aventas  Areas que evalva Abtenticación y autorización  13 Politicas de control de acceso y persión de Registro y monitoreo de acceso y persión de acceso y per	Obsetiva:  VIdentificar vulnerabilidades evaluar politicas de segundad verificar el complimiento de normativas i prevent acceso no autorizado  Areas que evalua  Control de acceso Protección de datos Configuraciones de la red Monitoreo y respuesta a incidentes  Tipo de auditoria Auditoria a controles de acceso a sistemas  Osectivo  Coetavar la efectividad de las medidas de seguridad implementadas para protegés la información y recursos de una organización  12 Gestión de ascerco y acentos Areas que evalva  Políticas de control de acceso y períod  14 Registro y monitoreo de acceso  Tipo de auditoria Auditoria de Informativa Forense  VIdentificar y documentar actividades illegales o frauditeritas en la empresa  Rewoilur y preservar proebas concretas para  Su aro en el proceso  Areas que evalva - Almacenamiento de datos	Curso : By "A"	Huerla Anglie Elizabeth
Areas que evalva estado de acceso a sistemas  Control de acceso protección de datas  Configuraciones de la real  Monitoreo y respuesta a inicidentes  Tipo de auditoria Auditoria a controles de acceso a sistemas  Corectivo Evalvar la efectividad de las medidas de seturidad implementadas para proteger la información y recursos de una organización  12 Gestión de uscarios y autorización  13 Gestión de uscarios y autorización  14 Gestión de uscarios y autorización  15 Políticas de control de acceso y período 15 Políticas de control de acceso y período 15 Políticas de control de acceso y período 15 Registro y monitoreo de acceso  Tipo de auditoria Auditoria de Informativa Forense  « Identificar y documentar actividades illegutes o frauditerilas en la empresa 18 Recopitar y preservar probas concretas por 18 Su oso en el proceso  Sistemas Operativos  - Redes - Almacenamiento de datos	Areas que evalva esculva de acceso de acceso a sietemas  Control de acceso de la rea  Protección de clatos Configuraciones de la rea  Monitoreo y respuesta a incidentes  Tipo de auditoria Auditoria a controles de acceso a sietemas  Cosectivo  Evalvar la efectividad de las medidas de seguridad implementadas para proteger la información y recursos de una organización  Areas que evalva especial y autorización  Politicas de acorrol de acceso y período de Registro y monitoreo de acceso y período de Registro y monitoreo de acceso  Tipo de auditoria Auditoria de Informativa Forense  * Identificar y documentar actividades ilea gues o fravalutentas en la empresa en Rewellar y preservar puebas concretas para su oro en el proceso  Sistemas Operativos  - Redes  - Almacenamiento de datos	Tipo de auditaria:	Auditorio de seguridad de redes
Protección de datos Configuraciones de la red Monitoreo y respuesta a inicidentes  Tipo de auditoria Auditoria a controles de acceso a sistemas  Ovectivo  © Evalvar la etectividad de las medidas de seguridad implementadas para proteges la información y recursos de una organización  12 Gestión de uscarios y cuentas  Areas que evalva 2ª Avienticación y autorización se Políticas de centrol de acceso y pernico 4º Registro y monitoreo de acceso y pernico  12 Auditoria de Informativa Actividades ille.  Quies o fraudotentas en la empresa e Rewpilar y preservar pruebas concretas para su oso en el proceso  Sistemas Operativos  Redes  Almacenamiento de datos	Protección de datos Configuraciones de la red Monitoreo y respuesta a incidentes  Tipo de auditoria Auditoria a controles de acceso a sistemas  Obectivo  © Evalvar la efectividad de las medidas de seguridad implementadas para proteger la información y recursos de ona organización  12 Gestión de uscarios y aventas  Areas que evalva « Aventicación y autorización » Políticas de control de acceso y pernico   12 Registro y monitoreo de acceso y pernico   13 Auditoria de Informativa Forense  14 Identificar y documentar actividades ilegules o fraudotentas en la empresa   15 Rewpilar y preservar proebas concretas para   15 Sistemas Operativos  16 Redes  Almacenamiento de datos	Opzetino:	politicas de segundad verificar el complimiento
Objectivo  © Evalvar la efectividad de las medialas de seguridad implementadas para proteger la información y recursos de una organización  1º Gestión de usuaras y cuentas  Areas que evalvo   Politicas de control de acceso y premios  Registro y monitoreo de acceso  Tipo de auditoria Auditoria de Informativa Forense  Identificar y documentar actividades ile.  gales o fraudolentas en la empresa  Rewpilar y preservar proebas concretas para  Su oso en el proceso  Sistemas Operativos  Pedes  Almacenamiento de datos	Objectivo  © Evaluar la efectividad de las medidas de seguridad implementadas para proteger la información y recursos de una organización  1º Gestión de usuaras y autorización  Areas que evalua el Autentitución y autorización  8º Politicas de acreso y premiso no Registro y monitoreo de acreso y premiso no Registro y monitoreo de acreso  Tipo de auditoria el Informativa Forense  * Identificar y documentar actividades ilegales o fraudotenhas en la empresa el Rewillar y preservar pruebas concretas para su aso en el proceso  Sistemas Operativos  - Cedes - Almacenamiento de datos	Áreas que evalva	· Protección de datos · Configuraciones de la red
Selvicidad implementadas para proteges la información y recursos de una organización  12 Gestión de usuarios y cuentas  Areas que evalóa 29 Autenticación y autorización 52 Politicas de control de acceso y premiso 42 Registro y monitoreo de acceso 42 Registro y monitoreo de acceso 43 Porense 44 Auditoria de Informativa Actividades ile.  Sules o fraudulentas en la empresa 42 Rewpillar y preservax pruebas concretas para 50 uso en el proceso 50 uso en el proceso 50 de acceso 63 de acceso 64 de acceso 65 de acce	Seguridad implementadas para protegés la información y recursos de una organización  12 Gestión de usuarios y aventas  Areas que evalúa 29 Autenticación y autorización 50 Políticas de control de acceso y premiso 10 Registro y monitoreo de acceso y premiso 10 Registro y monitoreo de acceso 10 Registro y monitoreo de acceso 10 Registro y documentas actividades ile.  3 Identificar y documentas en la empresa 10 Rewpilar y preservar pruebas concretas para 10 su oso en el proceso 10 Sistemas Operativos 10 Redes 10 Re	Tipo de auditoria	Auditoria a controles de acceso a sistemas
Areas que evalva de Autenticación y autorización se Politicas de control de acceso y premios registro y monitores de acceso de	Areas que evalva 2ª Autentituación y autoritación 5º Politicus de control de acceso y premios 1º Registro y monitores de acceso  Tipo de auditoria Auditoria de Informatica Forense  * Identificar y documentar actividades ile- gules o fraudulentas en la empresa * Rewpilur y preservax pruebas concretas para su uso en el proceso  - Sistemas O perativos - Redes - Almacenamiento de datos	Objectivo	seguridad implementadas para proteges la
* Identificar y documentar actividades ile.  gules o fraudulentas en la empresa  Rewpilar y preservar pruebas concretas pan  su uno en el proceso  Sistemas Operativos  - Redes  reas que evalva - Almacenamiento de datos	* Identificar y documentar actividades ile.  gules o travdulentas en la empresa  * Reapillar y preservar pruebas concretas para  su uso en el proceso  - Sistemas O perativos  - Redes  - Redes  - Almacenamiento de datos	Areas que evalóa	2º Autenticución y autorización 3º Políticus de control de acceso y premios
gules o fraudulentas en la empresa  * Rewpillur y preservar pruebas concretas para su uno en el proceso  - Sistemas Operativos  - Redes  - Redes	gules o fraudulentas en la empresa  * Rewpilur y preservar pruebas concretas para su uso en el proceso  - Sistemas O perativos  - Redes  - Redes	Tipo de auditoria	Auditoria de Informatica Forense
treas que evalva - Almace numiento de datos	Areas que evalva - Almacenamiento de datos		* Rewpilar y preservar pruebas concretas para
Circo Ciedi Girias		treas que evalua	- Redes - Almacenamiento de datos

Tipo de auditoria	Auditoria de seguridad de sitio web			100	
Objetivo	Prevenir y reducir les neogo que pueden efectuar la confidencialidad, la integridad y la disponibilidad del sitio web.				
Area evalua	Codigo, componetes, seguridad perimental protocolo de seguridad				
Tipo de auditoria	Hacking etico				
objetivo	VIdentificar vulnerabiliad en los sistemus aplicacione y redes para facilitar la seguridad y prevenir			5	
Area evolour	- Redes - Aplicacione web - Sistema operativo - Politicus internus	1	1	C	9-202