**UNIVERSIDAD TECNOLÓGICA NACIONAL**

**FACULTAD REGIONAL RESISTENCIA**

Icono

Descripción generada automáticamente

**Administración de Sistemas de Información**

**Trabajo Práctico 3.2 - Auditoría de Sistemas**

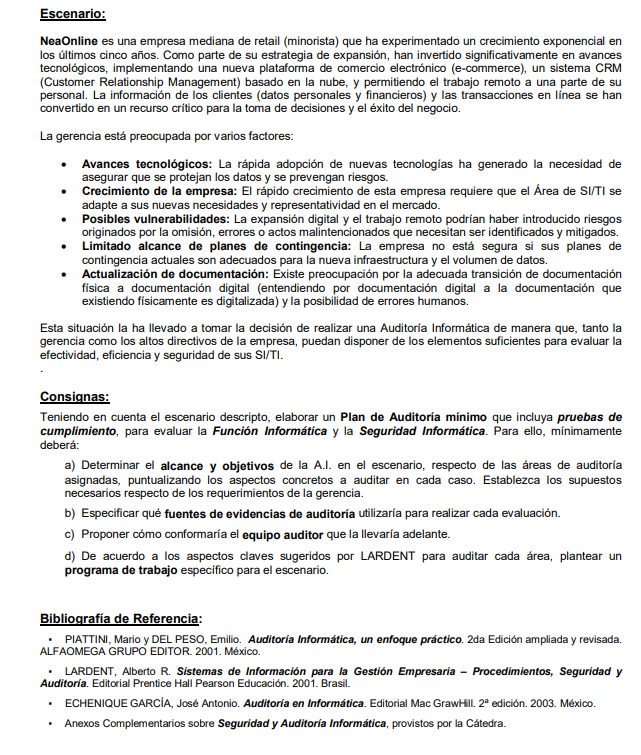
**Año:** 2025

**Profesores:**

* Claudia Alejandra Soria Ojeda
* Raúl Alejandro Montiel
* Rosina Sonia Analía Ramírez

**Integrantes:**

* Aguirre, Amilcar Nicolás
* Drose, Juan Ignacio
* Rivero, Bruno Sebastian
* Rosin, Zaira Antonella
* Sáez, Juliana
* Suarez, Tomás Alfonso



**Supuestos:**

-Se tiene en cuenta que la empresa NEONLINE no está desarrollando actualmente ningún sistema adicional, y solo cuentan con los mencionados CRM e e-commerce

- El sistema CRM basado en la nube empleado por la empresa es proveído por contrato/licencia de uso.

# 

# **A. Alcances y objetivos según áreas de auditoría**

**1 - Evaluación de la función informática (organización y administración del ambiente informático)**

Objetivos:

* Examinar la documentación física y digital existente y evaluar el nivel de actualización de esta última.
* Verificar que la estructura organizativa asegure una adecuada separación de funciones para cumplir con principios de control interno.
* Verificar la presencia de un buen diseño de control interno a causa de acotar las deficiencias y riesgos de procesamiento.
* Analizar el nivel de formación del personal y evaluar si por medio del mismo se alcanzan los estándares diseñados.
* Examinar si existen estándares de actuación y evaluar su adecuación y vigencia.

Alcance:

* Documentación normativa asociada al área de SI/TI (reglas/pautas empleadas en el ámbito de trabajo, procesos operativos, etc)
* Relevamiento de la documentación asociada a la infraestructura empleada de SI/TI
* Documentación física y digital
* Controles internos del procesamiento de la información
* Perfiles profesionales de los empleados del área de SI/TI y planes de capacitación

**2 - Evaluación de la seguridad informática**

Objetivos**:**

* Verificar la protección de los activos críticos para la organización.
* Analizar el cumplimiento de la legislación aplicable así como de las políticas y normas internas.
* Examinar si existe una evaluación periódica y adecuada de riesgos.
* Asegurar los accesos lógicos al sistema CRM de la nube
* Evaluar la correcta correcta implementación de los diferentes medidas de seguridad
* Evaluar las medidas de seguridad implementadas en la organización
* Determinar la capacitación de los empleados de las diferentes medidas y las políticas de seguridad implementadas
* Evaluar la adecuación de los planes de contingencia determinados

Alcance**:**

* Protección de los activos críticos, en particular los datos personales y comerciales de clientes y proveedores.
* Documentación depolíticas internas de seguridad, estándares, procedimientos y normativas vigentes en materia de protección de la información.
* Accesos lógicos al sistema CRM basado en la nube
* Documentación de medidas de seguridad implementadas
* Programas de formación existentes en relación con la seguridad de la información y el cumplimiento de las políticas internas.
* Documentación planes de contingencia y recuperación ante desastre**s**
* Documentación de las evaluación de riesgos,

# **B. Fuentes de evidencia según cada evaluación**

1. Evaluación de la función informática:

* Políticas y procedimientos establecidas en el área de SI/TI
* Código de conducta
* Organigrama del área de SI/TI
* Descripciones de puestos del área
* Plan estratégicos de TI
* Documentación sobre la plataforma de e-commerce
* Registro de capacitación de empleados
* Entrevistas a los empleados del área SI/TI sobre función informática
* Informes de Auditorías pasadas

1. Evaluación de la seguridad informática:
   * Políticas y normas de seguridad de la información
   * Inventarios de activos
   * Documentación de planes de contingencia
   * Documentación de medidas de seguridad aplicadas
   * Procedimientos de gestión de accesos lógicos y físicos
   * Bitácoras de acceso lógico y físico
   * Reportes de incidentes de seguridad
   * Evaluaciones de cumplimiento de normativas de seguridad
   * Entrevistas a los empleados del área SI/TI sobre seguridad informática
   * Informes de Auditorías pasadas

# **C. Equipo Auditor**

El equipo auditor comprobará que en el procedimiento de adquisición se valoran aspectos relativos a la necesidad real de los equipos solicitados y a la integración de dichos equipos con el sistema existente.

* **Jefe de departamento de Auditoría / Auditor líder:** es el responsable de:
  + Planificar, organizar, dirigir y evaluar la auditoría.
  + Coordina las actividades del equipo y asegura que se cumplan los objetivos.
  + Diseña el plan de trabajo.
  + Define metodologías, tareas, metas y formación del equipo.
* **Auditor interno de TI / auditores expertos**: Actúa como consultor, ofreciendo ideas y apoyo, tiene un papel constructivo y colaborativo. Es responsable de:
  + Crear metodologías necesarias para auditar las distintas áreas.
  + Aporta sugerencias para establecer procedimientos de seguridad, control interno, efectividad y eficacia y medición del riesgo empresarial.
  + Ejecuta las auditorías
* **Gerente o supervisor de auditoría:** Realiza los programas de trabajo, dirige y supervisa directamente a las personas en cada uno de los trabajos de los que es responsable. Entroncando los conceptos de valor añadido y gestión del cambio dentro de su trabajo. Es el que más "vende" la función con el auditado.
* **Expertos técnicos:** Aportan conocimientos especializados en áreas relevantes para la auditoría, como tecnología, finanzas, o aspectos legales.

**Responsabilidades**: El tamaño sólo se puede precisar en función de los objetivos de la función. pero en mi opinión, para una organización tipo, el abanico de responsabilidades debería cubrir

* Especialista en el entorno informático a auditar y en gestión de bases de datos.
* Especialista en comunicaciones y/o redes.
* Responsable de gestión de riesgo operativo y aplicaciones.
* Responsable de la auditoría de sistemas de información, tanto en explotación como en desarrollo.
* En su caso, especialista para la elaboración de programas de trabajo conjuntos con la Auditoría financiera.

El equipo auditor supone un auditor líder y una diferenciación en dos equipos de auditorías específicos a auditar:

1. Laura Fernández

**Cargo institucional:** Jefa de Control Interno

**Rol en la auditoría:** Auditora Líder / Jefa del Departamento de Auditoría

**Responsabilidades específicas:**

* Planificación, organización y dirección integral de la auditoría.
* Definición del plan de trabajo, metodología, metas y alcance.
* Coordinación general de actividades del equipo auditor.
* Validación de hallazgos y aseguramiento del cumplimiento de los objetivos.
* Representación del equipo ante la Alta Dirección.

**Certificaciones relevantes:**

* ISO/IEC 27001 Lead Auditor (IRCA)
* CISA (Certified Information Systems Auditor – ISACA)

2. Juan Roman Riquelme

**Cargo institucional:** Analista de Procesos de TI

**Rol en la auditoría:** Supervisor de Auditoría de Sistemas de Información

**Responsabilidades específicas:**

* Dirección operativa del equipo asignado a la función informática.
* Elaboración de los programas de trabajo para esta área.
* Supervisión directa del relevamiento de documentación, control interno, estructura organizativa y formación del personal TI.
* Promotor de iniciativas de mejora continua y de alineación con estándares de calidad.

**Certificaciones relevantes:**

* COBIT 2019 Foundation (ISACA)
* ITIL v4 Foundation

3. Julian Álvarez

**Cargo institucional:** Analista Sr. de Aplicaciones de Negocio

**Rol en la auditoría:** Auditor Interno de TI / Especialista en Sistemas Aplicativos

**Responsabilidades específicas:**

* Ejecución de auditoría técnica sobre los sistemas instalados (CRM, plataforma e-commerce).
* Evaluación de procedimientos operativos, documentación técnica y actualización de los sistemas.
* Análisis de riesgos en la explotación de aplicaciones y propuesta de mejoras.

**Ámbito especializado:** Sistemas en explotación / bases de datos / software de gestión empresarial

**Certificaciones relevantes:**

* CISA (ISACA)
* Scrum Master Certified (SMC)

4. Carla Mendieta

**Cargo institucional:** Especialista en Calidad y Seguridad de TI

**Rol en la auditoría:** Auditor Interno de TI / Especialista en Seguridad Informática

**Responsabilidades específicas:**

* Evaluación de políticas y medidas de seguridad implementadas.
* Verificación de gestión de accesos lógicos (CRM en la nube), protección de datos y controles técnicos.
* Coordinación de entrevistas al personal para validar su conocimiento sobre normas de seguridad y continuidad.

**Ámbito especializado:** Seguridad informática / comunicaciones / control de acceso

**Certificaciones relevantes:**

* ISO/IEC 27001 Lead Implementer (PECB)
* CompTIA Security+

5. Sofía Ruiz

**Cargo institucional:** Ingeniera de Infraestructura y Continuidad

**Rol en la auditoría:** Auditor Interno de TI / Especialista en Riesgo Operacional y Continuidad de Negocio

**Responsabilidades específicas:**

* Evaluación de los planes de contingencia y recuperación ante desastres (DRP, BCP).
* Análisis de resiliencia operativa de la infraestructura de TI.
* Verificación de registros y evidencias de pruebas de continuidad.

**Ámbito especializado:** Riesgo operativo / continuidad / disponibilidad de servicios

**Certificaciones relevantes:**

* Certified Business Continuity Professional (CBCP)
* ISO/IEC 22301 Lead Implementer

6. Tomás de San Lorenzo de Almagro

**Cargo institucional:** Auxiliar Administrativo del Área de TI

**Rol en la auditoría:** Asistente de Auditoría / Documentador de Evidencias

**Responsabilidades específicas:**

* Recolección, ordenamiento y sistematización de las evidencias documentales.
* Trazabilidad entre los hallazgos y la documentación fuente.
* Apoyo logístico y operativo en entrevistas, reportes y cronograma.

**Certificación interna:**

* Curso de Formación Interna en Auditoría de Sistemas – Neo Online

# **D. Programa de trabajo**

| **1.1 PROGRAMA DE TRABAJO DE AUDITORÍA**  **1.1.a Área a auditar:** Evaluación de la función informática  **Objetivos:**   * Examinar la documentación física y digital existente y evaluar el nivel de actualización de esta última. * Verificar que la estructura organizativa asegure una adecuada separación de funciones para cumplir con principios de control interno. * Verificar la presencia de un buen diseño de control interno a causa de acotar las deficiencias y riesgos de procesamiento. * Analizar el nivel de formación del personal y evaluar si por medio del mismo se alcanzan los estándares diseñados. * Examinar si existen estándares de actuación y evaluar su adecuación y vigencia. | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **1.1.b Alcance:**   * Documentación normativa asociada al área de SI/TI (reglas/pautas empleadas en el ámbito de trabajo, procesos operativos, etc) * Relevamiento de la documentación asociada a la infraestructura empleada de SI/TI * Documentación física y digital * Controles internos del procesamiento de la información * Perfiles profesionales de los empleados del área de SI/TI y planes de capacitación | | | | | | | |
| **1.1.c Fuentes de evidencia:**   * Políticas y procedimientos establecidas en el área de SI/TI * Código de conducta * Organigrama del área de SI/TI * Descripciones de puestos del área * Plan estratégicos de TI * Documentación sobre la plataforma de e-commerce * Registro de capacitación de empleados * Entrevistas a los empleados del área SI/TI sobre función informática * Informes de Auditorías pasadas | | | | | | | |
| **1.1.d Herramientas a emplear**:   * Checklist de cumplimiento de protocolos/ procedimientos operativos según la documentación empleada * Checklist de protocolos operativos seguidos por los empleados, según grado de adecuación (adecuado, inadecuado, desactualizado, inservible) * Software para registro centralizado de entrevistas y observaciones de los empleados * SW de gestión de documental * SW para análisis organizativo y roles * SW para la gestión de competencias de empleados * SW control de versiones de sistemas * SW para la gestión de proyectos * Entrevistas guiadas y formularios a empleados * Manual de normativas del ambiente organizacional | | | | | | | |
| **N°** | **Actividad / Tarea** | **Objetivo específico** | **Alcance** | **Herramienta** | **Tipo de prueba** | **Fuente de evidencia** | **Responsables** |
| **1** | Revisión documental de políticas, procedimientos y manuales TI | Verificar la existencia y actualización de la documentación asociada a las tecnologías de la información empleadas | Documentación normativa y operativa | Checklist de políticas y/o documentación | Cumplimiento | Manuales, instructivos, procedimientos, documentación registrada de políticas de TI | Asistente de Auditoría  **+** Auditor interno de TI |
| **2** | Analizar versiones y vigencia de documentos digitales | Evaluar el nivel de actualización de la documentación | Documentación digital operativa | Software de gestión documental | Sustantiva | Historial de versiones, logs de SW de gestión documental | Auditor Interno de TI |
| **3** | Revisión del organigrama y organización de roles | Verificar la adecuación y concordancia de los roles y la organización en el ámbito laboral según la funcionalidad de cada empleado  (segregación de funciones l) | Organigram y funciones de TI | SW para análisis organizativo y roles | Cumplimiento | Organigrama, documentación con descripción de puestos | Supervisor de auditoría |
| **4** | Evaluación de la formación y perfil del personal | Verificar/Validar la adecuación y calidad del cumplimiento de tareas del personal | Perfil profesional y capacitaciones | Método empírico (observación del personal);  Entrevistas ; encuestas;  SW para gestion de competencias de empleados | Cumplimiento | Legajos, certificados, plan de formación, CV, certificaciones | Supervisor de Auditoría |
| **5** | Entrevistas al personal clave sobre estructura y documentación operativa | Obtener información cualitativa y cuantitativa de la percepción sobre la estructura organizativa y de los procesos operativos | Personal de TI involucrado en documentación y operación | Guía estructurada de entrevista | Sustantiva | Entrevista grabada o registrada; transcripciones de comentarios de personal | Auditor interno de TI+ Asistente de auditoría |
| **6** | Revisar si existen estándares de desempeño definidos y aplicables | Examinar existencia de estándares técnicos y operativos | Estándares de calidad/ Métricas operativas | SW de gestión de desempeño, empleando variables como KPis | Cumplimiento | Estándares de servicio, reportes mensuales | Auditor Interno de TI |

| **1.2 PROGRAMA DE TRABAJO DE AUDITORÍA**  **1.2.b Área a auditar:** Evaluación de la seguridad informática  **Objetivos:**   * Verificar la protección de los activos críticos para la organización. * Analizar el cumplimiento de la legislación aplicable así como de las políticas y normas internas. * Examinar si existe una evaluación periódica y adecuada de riesgos. * Asegurar los accesos lógicos al sistema CRM de la nube * Evaluar la correcta correcta implementación de los diferentes medidas de seguridad * Evaluar las medidas de seguridad implementadas en la organización * Determinar la capacitación de los empleados de las diferentes medidas y las políticas de seguridad implementadas * Evaluar la adecuación de los planes de contingencia determinados | | | | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **1.2.b Alcance:**   * Protección de los activos críticos, en particular los datos personales y comerciales de clientes y proveedores. * Documentación depolíticas internas de seguridad, estándares, procedimientos y normativas vigentes en materia de protección de la información. * Accesos lógicos al sistema CRM basado en la nube * Documentación de medidas de seguridad implementadas * Programas de formación existentes en relación con la seguridad de la información y el cumplimiento de las políticas internas. * Documentación planes de contingencia y recuperación ante desastre**s** * Documentación de las evaluación de riesgos, | | | | | | | |
| **1.2.c Fuentes de evidencia:**   * Políticas y normas de seguridad de la información * Inventario de activos * Documentación de planes de contingencia * Documentación de medidas de seguridad aplicadas * Procedimientos de gestión de accesos lógicos y físicos * Bitácoras de acceso lógico y físico * Documentación de capacitación de empleados * Reportes de incidentes de seguridad * Evaluaciones de cumplimiento de normativas de seguridad * Entrevistas a los empleados del área SI/TI sobre seguridad informática * Informes de Auditorías pasada | | | | | | | |
| **1.2.d Herramientas a emplear**:   * Checklist de control de cumplimiento de políticas de seguridad * SW para el análisis de vulnerabilidades * SW de gestión documental de evidencias y normativas * Formularios estructurados para entrevistas * Herramienta de auditoría de políticas de backup. * Herramienta para el análisis de logs * SW para la gestión de accesos a los sistemas * SW tipo Firewall para la defensa contra malwares | | | | | | | |
| **Nro** | **Actividad /Tarea** | **Objetivo específico** | **Alcance** | **Herramienta** | **Tipo de prueba** | **Fuente de evidencia** | **Responsables** |
| **1** | Análisis de activos de la organización | Determinar activos de la organización | Documentación de de activos | Checklist y/o documentación | Sustantiva | Inventarios de activos | Auditor interno |
| **2** | Análisis de los medios de seguridad empleados | Determinar los medios de seguridad empleados | Documentación de medidas de seguridad | Checklist y/o documentación | Cumplimiento | Documentación de medidas de seguridad aplicadas | Auditor interno |
| **3** | Análisis de normas y políticas de seguridad | Determinar las normas y políticas de seguridad | Documentación de políticas de seguridad de la información | Checklist y/o documentación | Cumplimiento | Políticas de seguridad de la información | Supervisor de auditoría |
| **4** | Análisis de evaluación periódica de seguridad | Determinar si existe, de que tipo y como se realiza la evaluación periódica de seguridad | Documentación políticas y normas de seguridad y activos de la empresa | Checklist y/o documentación | Cumplimiento | Políticas de seguridad de la información  Inventario de activos  Documentación de medidas de seguridad aplicadas | Auditor interno |
| **5** | Revisión de accesos lógicos y físicos | Determinar los accesos lógicos y físicos a la CRM y plataforma e-commerce | Documentación de los accesos físicos y lógicos | SW de análisis de accesos lógicos y SW de análisis de accesos físicos | Sustantiva | Procedimientos de gestión de accesos lógicos y físicos  Bitácoras de acceso lógico y físico | Asistente de auditoría |
| **6** | Revisión de capacitación de empleados a aspectos de seguridad | Determinar qué tipo de capacitación de seguridad tienen los empleados | Documentación de capacitación de empleados | Checklist y/o documentación | Cumplimiento | Documentación de capacitación de empleados | Supervisor de auditoría |
| **7** | Análisis de planes de contingencia | Determinar los diferentes planes de contingencia | Documentación de planes de contingencia | Checklist y/o documentación | Cumplimiento | Documentación de planes de contingencia | Auditor interno |
| **8** | Revisión de adecuación de seguridad aplicada a los activos | Analizar la adecuación de las medidas de seguridad aplicada según cada activo | Documentación políticas y normas de seguridad y activos de la empresa | SW para análisis de adecuación de seguridad aplicada a los activos | Sustantiva | Políticas de seguridad de la información  Inventario de activos  Documentación de medidas de seguridad aplicadas | Auditor interno |
| **9** | Revisión de adecuación de planes de contingencia | Determinar la adecuación de los planes de contingencia según los activos | Documentación de planes de contingencia | SW para análisis de adecuación de planes de contingencia a activos | Sustantiva | Planes de contingencia | Auditor interno |
| **10** | Evaluación de cumplimiento de las normas y políticas de seguridad | Analizar por un periodo de tiempo el comportamiento de los empleados según las diferentes normas y políticas de seguridad | Documentación políticas y normas de seguridad | Método empírico (observación del personal) | Cumplimiento | Políticas y normas de seguridad de la información  Evaluaciones de cumplimiento de normativas de seguridad | Asistente de Auditoría |
| **11** | Revisión del correcto uso de la evaluación periódica de seguridad | Análisis del uso de la evaluación periódica de seguridad | Documentación políticas y normas de seguridad | Checklist y/o documentación  SW para analizar el correcto uso de la evaluación periódica | Cumplimiento | Políticas y normas de seguridad de la información  Documentación de planes de contingencia  Documentación de medidas de seguridad aplicadas | Supervisor de auditoría |
| **12** | Entrevistas a los empleados sobre capacitación en seguridad | Determinar el conocimiento de los empleados sobre temas referidos a la seguridad | Empleados del área SI/TI sobre | Guía estructurada de entrevista | Sustantiva | Entrevistas a los empleados del área SI/TI sobre seguridad informática | Auditor interno |
| **13** | Revisión de anteriores violaciones de seguridad | Controlar las causas y las respuestas a las anteriores violaciones de seguridad | Documentación sobre cualquier incidente de seguridad | SW para analizar las violaciones de seguridad | Sustantiva | Reportes de incidentes de seguridad | Auditor interno |
| **14** | Entrevistas de empleados sobre seguimiento de medidas de seguridad | Determinar según las opiniones de los empleados el seguimiento correcto de las medidas de seguridad | Empleados del área SI/TI sobre | Guía estructurada de entrevista | Sustantiva | Entrevistas a los empleados del área SI/TI sobre seguridad informática | Asistente de Auditoría |
| **15** | Entrevistas a empleados sobre planes de contingencia | Determinar el conocimiento y preparación de los empleados a los planes de contingencia activos | Empleados del área SI/TI sobre | Guía estructurada de entrevista | Cumplimiento | Entrevistas a los empleados del área SI/TI sobre seguridad informática | Auditor interno |