# INTRODUCCIÓN:

En este informe se desarrollarán los aspectos a tener en cuenta en la auditoría de la empresa diario UNO, y son los siguientes:

* Seguridad personal
* Seguridad física y ambiental
* Seguridad lógica
* Cumplimiento de la ley de seguridad

# OBJETIVO:

Auditar a la empresa diario UNO, en lo que respecta a todo el sector del área de sistemas, en los aspectos previamente mencionados.

# SEGURIDAD PERSONAL

1. ¿Quién es el encargado de dar de alta o baja contraseñas y otros derechos de los usuarios?, ¿cada cuánto se controla?
2. ¿Quién verifica el correcto uso de PCs o impresoras utilizadas en la empresa, y cada cuánto tiempo?
3. ¿Quién verifica que los usuarios realicen sus capacitaciones en cuanto a la seguridad de la información y el uso de equipos?

# SEGURIDAD FÍSICA

**Las principales amenazas que se prevén en Seguridad Física son:**

* **Desastres naturales, incendios accidentales, tormentas e inundaciones**
* **Amenazas ocasionadas por el hombre**
* **Disturbios, sabotajes internos y externos deliberados.**

**Evaluar y controlar permanentemente la seguridad física de las instalaciones de**

**cómputo y del edificio es la base para comenzar a integrar la seguridad como una**

**función primordial dentro de cualquier organismo.**

**Tener controlado el ambiente y acceso físico permite:**

* **Disminuir siniestros**
* **Trabajar mejor manteniendo la sensación de seguridad**
* **Descartar falsas hipótesis si se produjeran incidentes**
* **Tener los medios para luchar contra accidentes**

Para evaluar el control que se tiene sobre los riesgos y peligros que se puedan presentar en cuanto a la seguridad física, se utilizan las siguientes preguntas:

1. ¿Dónde y con qué frecuencia se capacitará al personal en cuanto al uso de matafuegos?
2. ¿Qué tipos de matafuego van a ser utilizados para la protección de los bienes de la empresa?
3. ¿Dónde se almacenan las cintas de backUp, con qué frecuencia se implementan y qué tipo de backUps se realizan?
4. ¿En qué lugar se encuentra el sistema de aire acondicionado y qué tipo de sistema seria? , detallar.
5. ¿Dónde estaría ubicado el generador de energía?,¿Quién es el encargado de operarlo?
6. ¿Se realiza un plan de seguridad física contra catástrofes como: inundaciones, incendios, cortes de energía?
7. ¿Existe un ente encargado para dar solución a los distintos incidentes de seguridad en cada area?
8. ¿Existe algún análisis de riesgos en la organización?
9. ¿Existe un adecuado control acerca del HW que entra y sale de la empresa?

## SEGURIDAD LÓGICA

**Las principales amenazas que se prevén en Seguridad Logica son:**

• Chantaje/espionaje empresarial

• Divulgación/robo/manipulacion de información confidencial

. Robo de SW empresarial

1. **Tener un control sobre la seguridad lógica nos permitira:**

**1. Restringir el acceso a los programas y archivos**

**2. Asegurar que los operadores puedan trabajar sin una supervisión minuciosa**

**y no puedan modificar los programas ni los archivos que no correspondan.**

**3. Asegurar que se estén utilizando los datos, archivos y programas correctos**

**en y por el procedimiento correcto.**

**4. Que la información transmitida sea recibida por el destinatario al cual ha**

**sido enviada y no a otro.**

**5. Que la información recibida sea la misma que ha sido transmitida.**

**6. Que existan sistemas alternativos secundarios de transmisión entre**

**diferentes puntos.**

**7. Que se disponga de pasos alternativos de emergencia para la transmisión**

**de información.**

Se auditará el control y prevenciones lógicas que se plantearon en el desarrollo del plan de la empresa diario UNO. Los siguientes puntos nos servirán de base para poder corregir o mejorar ciertos puntos antes que generen conflictos:

1. ¿Cómo se tiene acceso al servidor?, ¿Es posible acceder remotamente?
2. En cuanto a los administradores ¿Cómo será el perfil de los mismos? ¿Se definen algunos permisos sobre el Servidor y la Base de datos?
3. En cuanto al Firewall, ¿cómo se implementará?
4. En cuanto a los backups, ¿mediante qué medio se realizará? ¿Dónde se guardarán los mismos, y quién será el responsable?
5. ¿Se cuenta con un sistema de control de acceso y autorización de la informacion? Los privilegios de acceso, ¿sobre qué usuarios se aplicarían?
6. ¿Utilizan algún algoritmo de encriptación de claves? ¿Qué tipo de datos se encriptarán?
7. ¿En caso de encontrar infecciones en las computadoras, qué medidas se toman?
8. ¿Existen políticas para el manejo de Internet?
9. ¿Existen políticas para el manejo de redes, sistemas operativos, aplicaciones, etc.?
10. ¿Se mantiene un registro de las actividades que los Administradores y usuarios realizan sobre un sistema?

## CUMPLIMIENTO DE LA LEY DE SEGURIDAD

### CONTROL DE SEGURIDAD CONTRA INCENDIOS Y OTROS DESASTRES

Área donde ocurrió, responsable, situación en la que se produjo el accidente, modo en el que se procedió.

1. ¿Quién dictará las capacitaciones para el uso de matafuegos?,¿Cada cuánto se harán, y a quiénes se capacitará?
2. ¿Se realizarán controles sobre alarmas y extintores de humo en mantenimiento?, En caso afirmativo, ¿Cada cuánto?
3. ¿La señalización será impuesta siguiendo las pautas de alguna norma? ¿Y qué sucederá con el uso de matafuegos y su posicionamiento?
4. ¿Quiénes estarán encargados del mantenimiento de la infraestructura?
5. ¿Cada cuánto tiempo se realizarán los simulacros? ¿Quién será el encargado de realizarlos?
6. ¿Quiénes conocerán los códigos de las alarmas y estarán habilitados para activarlas y desactivarlas? ¿Quién se hará cargo de las cámaras de seguridad?

# CONCLUSIONES