**Seguridad 360°**

# ¿Qué es Seguridad 360°?

**Seguridad 360°** es una estrategia enfocada en soluciones de seguridad que se obtiene, 1ro, con un análisis global de todas las fuentes de información relevantes que informan o advierten de posibles incidentes y, después aplicando una respuesta conforme al protocolo establecido para cada tipo de incidente, que consisten en medidas preventivas o correctivas ante las amenazas. Todo esto teniendo en cuenta la seguridad de todas las áreas del cliente que deben ser protegidas.

En este proceso, **todos los departamentos**, en mayor o menor medida, se encuentran implicados en la seguridad de las compañías, podemos destacar por ejemplo:

* Seguridad física
* RRHH
* Riesgos laborales
* Calidad
* Mantenimiento
* Informática
* Ciberseguridad
* Inteligencia Empresarial

# Gestión de Incidencias

A la hora de reducir incidentes, accidentes, situaciones inseguras, consecuencias no deseadas en una institución educativa o en una organización laboral se proponen 3 ejes de estudio y análisis:

1. Explorar la base de los comportamientos individuales, organizacionales y de liderazgo.
2. Desarrollar un modelo mental proactivo para detectar situaciones inseguras y riesgos.
3. Sincronizar a todas las áreas organizativas en la prevención de situaciones inseguras.

A través de dicha actividad se propone:

* Influir en la concientización sobre la falibilidad y vulnerabilidad humanas.
* Suministrar herramientas conductuales preventivas.
* Presentar un modelo mental proactivo hacia la identificación de situaciones de inseguridad.
* Facilitar la comunicación entre los compañeros para reconocer errores humanos y situaciones inseguras.

# Gestión de Incidencias y Ciclo de la Inteligencia

Este proceso se realiza en 5 fases:

## 1) Planificación

La planificación y la dirección implican la gestión de todo el esfuerzo de inteligencia, desde la identificación de la necesidad de datos, hasta la entrega de un producto de inteligencia a un consumidor.

Forman parte tanto del comienzo como del final del ciclo, debido a que comprometen, por una parte, la **formulación de requisitos específicos de recolección, procesamiento, análisis y difusión**; y por otra, porque la inteligencia completa, debe respaldar la toma de decisiones y, además, la acción genera con frecuencia nuevos requisitos de información.

Todo el proceso depende de la guía del consumidor, el usuario final, de la inteligencia. Se puede decir que el proceso de inteligencia es impulsado por el consumidor.

Además, los responsables de formular políticas, los directivos y los directores de seguridad, tienen diferentes necesidades de información.

## 2) Obtención de la información

La obtención de la información está esparcida en muchos departamentos y sistemas de información, y también en fuentes externas. Debemos tener en cuenta que:

* Normalmente se subestiman las fuentes abiertas, pero son fuentes importantes.
* Existen fuentes confidenciales que deben ser consideradas.
* La integración de todas estas fuentes es un paso obligado para tener una visión de conjunto, y las interrelaciones entre los datos.

## 3) Análisis de la información

Al disponer de múltiples fuentes de información, es necesario traducir cada información, cada incidente detectado a un mismo lenguaje, puesto que en la seguridad es crítica la respuesta a tiempo.

## 4) Diseminación

En función de los medios disponibles, se gestionará la respuesta, que tiene necesidad de una **retroalimentación constante** para comprobar que la inteligencia es correcta, comprobando en tiempo real los datos para refinar el análisis y despachar los recursos conforme a la evolución del incidente.

## 5) Revisión

En esta etapa es donde se **consolidan los protocolos a aplicar en función del tipo de incidente**. Mediante una constante revisión de los protocolos, se podrán ajustar a las condiciones de los incidentes, para obtener el éxito en las respuestas.

Por ejemplo, en una empresa, debe ser la Dirección quien lidere en esta fase, puesto que implica a todas las áreas funcionales.

En definitiva, de manera que se pueda llevar a cabo una correcta gestión de incidentes, es imprescindible que se haga un uso de un **formato único de incidente y de base de datos** para referirnos a las distintas infraestructuras o activos de la empresa (mapa, planos, diagramas de red, flota de vehículos, etc.) de forma que englobe a todas las áreas: Riesgos Laborales, Producción, Informática, Ciberseguridad y Seguridad, entre otros.

# Desempeño Humano

El desempeño humano es un sistema que comprende una red de elementos asociados, ejecutados por un individuo para lograr objetivos referidos a una actividad específica que trabajan juntos para producir resultados repetibles preestablecidos por una norma, protocolo o estándar. Abarca factores organizativos, condiciones del lugar de trabajo, comportamiento individual y resultados.

El enfoque del sistema pone una nueva perspectiva sobre el error humano, no es una causa de falla, por si sola, sino mas bien el efecto o síntoma de problemas más profundos en el sistema.

El error humano no es aleatorio; es conectado sistemáticamente a las características de las herramientas de las personas, las tareas que realizan y el funcionamiento del entorno en el que trabajan.

## ¿Error o violación?

**Error**: es una acción que se desvía no intencionalmente de un comportamiento esperado de acuerdo con algún estándar. Hay 2 tipos de errores: **Activos** y **Latentes**.

Los “activos” son errores que cambian el estado del equipo o sistema disparando inmediatamente consecuencias indeseables. Los “latentes” son debilidades no detectables relacionadas con la organización o con el equipo defectuoso.

**Violación**: involucra una desviación deliberada del comportamiento esperado.

La diferencia es que el error involucra problemas con el procesamiento mental de la actividad o con la información relacionada de trabajo. En cambio, la violación involucra factores motivacionales característicos del individuo o de la organización.

Los eventos pueden ser evitados por medio del entendimiento de las causas que los generaron y también por la transmisión de la experiencia operativa.

# Culpa

Culpar a las personas por sus errores tiene poco efecto en la prevención del error. Culpar continuamente a los trabajadores de las causas de los errores deja malas consecuencias.

**Ciclo de culpa**

Error humano.

Individuos discriminados.

Confianza reducida.

Menos comunicación.

La dirección vigila menos las condiciones en el lugar de trabajo.

Persistencia de las debilidades latentes de la organización.

Más defensas defectuosas y precursores del error.

# 9 Técnicas de Prevención del Error

## 1) Utilización de procedimientos

Existen normas y procedimientos que regulan todas las tareas. Conocerlos y cumplirlos reduce la posibilidad de cometer errores.

* Utilizar siempre el procedimiento adecuado en su última versión.
* Los jefes y líderes deben darlos a conocer.
* Los procedimientos y normas permiten dirigir la realización de tareas y disminuyen las situaciones propensas a error.

## 2) Auto-verificación

Atraer e incrementar la atención en un mismo antes de realizar una tarea.

* Tomarse unos minutos para hacer una auto-observación cada día y asegurarse de que la atención está focalizada en la tarea.
* La auto-verificación o autochequeo permite la prevención del error humano.
* En el caso de necesitarlo, el colaborador puede utilizar las herramientas de Verificación Independiente y Revisión de Pares.

## 3) Reunión Pre-trabajo

Herramienta de comunicación entre las personas involucradas en una tarea o proyecto a desarrollar.

* Asegura el conocimiento y entendimiento de las funciones de cada uno, y de los procedimientos que regulan nuestras tareas.
* Define objetivos y establece secuencias.
* Se realiza antes de comenzar una tarea, luego de una interrupción significativa o ante cambio de colaborador. También cuando intervienen varios sectores en la misma labor.

## Reunión Pos-trabajo

Reunión que se realiza inmediatamente después de finalizada la tarea con los trabajadores que estuvieron directa o indirectamente involucrados.

* Se utiliza para verificar que los objetivos propuestos en la Reunión Pre-trabajo fueron alcanzados.
* También es útil para identificar debilidades o precursores de error encontrados.
* Nos permite realizar acciones proactivas para evitar un error que pueda desencadenar en un evento.

## Verificación Independiente

La implementan dos personas separadas en tiempo y espacio. El segundo individuo calificado realiza el chequeo de las tareas del primer individuo, en un momento posterior.

* Se utiliza para confirmar la condición de una tarea después de realizada, para la reducción de errores.
* El individuo asignado para realizarla debe mantener independencia para asegurar la integridad del proceso.
* Deberán ser alentados los aciertos y señalados los errores de una manera natural y permanente.

## 6) Revisión de Pares

Un compañero del ejecutor de una acción específica observa o chequea la misma, al miso tiempo que se está llevando a cabo e interviene si es necesario.

* Es conveniente que el compañero destinado a chequear quede designado en la Reunión Pre-trabajo.
* Sirve para ver los riesgos o las consecuencias potenciales que el ejecutor no ve.
* En toda tarea los intervinientes tienen dependencia mutua para reconocer situaciones propensas al error.

## 7) Comunicación Efectiva

Consiste en la transmisión de la información pertinente de manera precisa y frecuente asegurándonos de que el mensaje fue entendido en su totalidad.

* Se puede utilizar la técnica de las 3 Vías:
* 1ra. Emisor emite un mensaje.
* 2da. Receptor interpreta el mensaje y lo repite.
* 3ra. Emisor confirma si es correcto o no lo es.
* La comunicación abierta y efectiva es un recurso básico para prevenir errores en todo grupo y organización laboral.
* Es por sí sola la defensa más efectiva contra los eventos (WANO GL 2002).

## 8) Actitud Cuestionadora

Permite canalizar dudas y eliminar suposiciones a través de una crítica constructiva de procesos y procedimientos.

* Permite tomar conciencia sobre la incertidumbre y los riesgos potenciales.
* Facilita la búsqueda de la información requerida para realizar la tarea de una manera más segura.
* Promueve la Mejora Continua.

## 9) Toma de Decisiones

Cuando se toma una decisión, y las consecuencias de la misma no son claras, es necesario adoptar Decisiones Conservadoras.

* Usar toda la información disponible.
* Evitar las decisiones precipitadas o acciones apresuradas.
* Reducir al mínimo la incertidumbre y no proceder cuando es incierto.