INTRODUCCIÓN

El presente documento establece las acciones que se deben seguir para una adecuada prevención de los riesgos de robo, hurto y asalto, ya que el daño producido no solo afecta las finanzas y competitividad de las empresas, sino también el deterioro del ambiente de negocios por la incertidumbre de seguridad que se genera.

ASPECTOS GENERALES

Marco regulatorio

- Código Penal Costa Rica. Ley 4573
- Código Procesal Penal N° 7594
- Ley Contra la Delincuencia Organizada 8754
- Ley de protección a víctimas, testigos y demás sujetos intervinientes en el proceso penal, reformas y adición al Código Procesal Penal y al Código Penal Ley Nº 8720
- Manual sobre la aplicación eficaz de las Directrices para la prevención del delito. UNODC

OBJETIVO

El objetivo de esta guía es brindar los elementos de juicio necesarios para establecer un protocolo de prevención en caso de robo, hurto o asalto, así como, brindar apoyo a las empresas en la identificación de las medidas preventivas que faciliten su detección; y la promoción de una cultura de seguridad, para lo cual se deberá establecer las políticas, procedimientos y controles, que permitan identificar, medir, controlar y monitorear los riesgos de robo, hurto o asalto dentro de la organización.

La seguridad; por si misma NO ofrece protección absoluta, pero debe como mínimo conseguir los siguientes resultados:

- Dificultar la acción delictiva
- Retardarla, detectarla, localizarla.
- Impedir el libre desenlace de la actividad criminal.

APLICABILIDAD

Muchos expertos en seguridad han llegado a la conclusión que la mayor vulnerabilidad en la empresa esta justamente dentro de ella, es muy alto el porcentaje de robos, hurtos y estafas que se orquestan a lo interno, por lo que el plan de negocios debería contemplar una estrategia para implementar las medidas de prevención y seguridad correspondientes.

El peor enemigo de la seguridad es la idea de que "a mí nunca me sucede nada".

Otro aspecto importante es tener claro cuáles son las áreas vulnerables a este tipo de riesgos; de acuerdo con las operaciones o actividades; para lo cual se debe realizar un análisis del entorno, y evaluar la efectividad de las medidas preventivas implementadas.

DEFINICIONES

Robo: Es un delito contra el patrimonio, consistente en el apoderamiento de bienes ajenos de otras personas, empleando para ello la violencia o intimidación de las personas.

Hurto: Este delito consiste en tomar con ánimo de lucro cosas muebles ajenas contra la voluntad de su dueño, sin mediar la violencia o intimidación de las personas, es decir, generalmente el hurto se efectúa por descuido.

Asalto o atraco: Consiste en atacar por sorpresa a alguien con la misión de robarle sus pertenencias o dinero. Normalmente el asalto se perpetra con violencia y amenazas directas contra la vida de las personas, y haciendo uso de armas blancas o de fuego.

Prevención: Es la acción y efecto de prepararse con antelación a una determinada situación, implica el tomar las medidas preventivas necesarias y más adecuadas con el objetivo de contrarrestar un perjuicio o daño.

Medidas Preventivas: Son las acciones realizadas con el fin de eliminar o disminuir la probabilidad de materialización de los riesgos.

Riesgo: Probabilidad de ocurrencia de un evento originada por la exposición a una amenaza.
Amenaza: Elementos o factores que tienen la capacidad de causar un daño significativo (materialización de un riesgo).

Gestión de los Riesgos: Proceso sistemático, independiente y documentado para gestionar la identificación, clasificación, tratamiento, seguimiento, actualización y comunicación de los riesgos.

Conducta irregular: Acciones encaminadas a incumplir leyes, regulaciones, políticas internas, reglamentos o expectativas de las organizaciones u opuestas a la conducta ética empresarial y comportamientos no habituales.

Cibercrimen: Actividades ilícitas que se llevan a cabo para robar, alterar, manipular, enajenar o destruir información o activos (como dinero, valores o bienes desmaterializados) de compañías, valiéndose de herramientas informáticas y tecnológicas.

Política: Compromisos documentados, establecidos por la alta gerencia que representan lineamientos y son de carácter permanente.

Procedimiento: Documento que establece la metodología detallada para desarrollar una acción, debe indicar: qué se debe hacer, quién es responsable de hacerlo, cuándo debe hacerlo, cómo debe hacerlo y referencia a los registros que evidencien su cumplimiento.

Piratería: Obtención o modificación de información de otros, sin la debida autorización, ya sea una página web, una línea telefónica, computador o cualquier sistema informático de una entidad.

Vandalismo: Acciones físicas que atenten contra la integridad de los elementos informáticos, cuya finalidad es causar un perjuicio, como por ejemplo, la paralización de las actividades, como medio de extorsión o cualquier otro.

Brigada de Emergencia: Grupo seleccionado de personas que conforman una unidad, con conocimientos adecuados y debidamente capacitado para atender cualquier emergencia o siniestro dentro de las instalaciones.

Emergencia: se refiere a un suceso o acontecimiento que se presenta de manera fortuita y que, por lo general, requiere de algún tipo de acción para evitar o minimizar los daños, es una situación que exige la atención inmediata.

Delincuencia Organizada: es un grupo conformado por dos o más personas que existe durante cierto tiempo y que actúa concertadamente con el propósito de cometer uno o más delitos graves.

DESARROLLO DEL PROTOCOLO

Al identificar una situación sospechosa debe notificar inmediatamente al personal de vigilancia o Encargado de Seguridad de la empresa. A continuación, se listan algunos indicios o actos que pueden dar origen o requieren de revisiones particulares que ameritan el seguimiento:

- Visitantes, proveedores o funcionarios sin identificación visible o que se niegan a ser revisados por la seguridad.
- Presencia de individuos extraños merodeando por el lugar de trabajo.
- Personas con actitud sospechosa o nerviosas.
- Personas con la cara cubierta con pasamontañas, pañuelos, cascos, sombreros, anteojos obscuros, etc.
- Personas o funcionarios no autorizados en el área de trabajo, de acuerdo a las restricciones de acceso.
- Mallas, puertas, ventanas, candados o paredes con evidencia de haber sido forzadas o violentadas. En este caso no se debe de tocar o alterar la escena.
- Llamadas sospechosas o amenazantes.

Como identificar actividades sospechosas

- Si descubre que un proveedor o contratista que ha sido acusado de haber realizado este tipo de delitos.
- La no portación de una identificación válida o no es conforme al diseño utilizado por la empresa, funcionario, visitante, proveedor, o contratista.
- Vehículos sin matrícula, alterada o cubierta de alguna manera; o vehículos sospechosos.
- La negación por parte de visitantes o funcionarios para la revisión de efectos personales y/o vehículos al ingreso y salida de las instalaciones.
- Desvíos de la ruta preestablecida en caso de transporte de mercancía u otros bienes de le empresa.
- Llegadas tardías o retrasos imprevistos para que la persona no tenga el tiempo suficiente para cumplir cabalmente con el proceso que le corresponde.
- Obstrucción de investigaciones o la omisión deliberada de los controles, que mitigan este tipo de riesgos.
- La no aplicación de los procedimientos y controles definidos para mitigar los riesgos operativos.
- Fallas en el cumplimiento de las recomendaciones de los reportes de auditoría u omisiones en la implementación de estrategias sugeridas para evitar los riesgos.
- Fallas en la identificación de actividades o sitios en los cuales exista una alta exposición a este tipo de riesgos
- Malos tratos o censura a compañeros de trabajo que cumplan con su deber de reportar hechos sospechosos.
- Insistencia por parte de algún funcionario por querer ser parte de determinada tarea u operación, aunque no sea el rol que le corresponde.
- Fallas o falta de iluminación adecuada en las áreas.

- Puertas o ventanas abiertas cuando no deberían estarlo, según los horarios establecidos.
- Candados u otros dispositivos de seguridad abiertos cuando deberían permanecer cerrados.

MEDIDAS PREVENTIVAS

- Establecer procedimientos de selección y contratación de personal, con el fin de obtener funcionarios confiables, comprometidos y responsables.
- Establecer sistemas o mecanismos de identificación mediante gafetes con fotografía, códigos de identidad, claves y en general cualquier mecanismo que permita establecer en todo momento, quien es responsable, así como las horas de entrada y salida de cada persona.
- Establecer un programa de auditorias o inspecciones internas. Este control le permitirá detectar posibles acciones sospechosas o anómalas y tomar medidas de correctivas antes de que ocurra un evento.
- Establecer procedimientos control de documentos e información. No permitir que cualquiera tenga acceso abierto a toda clase de datos como clientes, productos, inventarios, precios, claves de acceso, información financiera y bancaria.
- Utilizar mecanismos de control formales y estrictos, sin la posibilidad de poder alterar sistemas y documentos.
- Capacitación del personal. Ejercicios prácticos o capacitaciones sobre cómo actuar en casos de situaciones críticas o como prevenir delitos.
- Protección de vehículos con sistemas de localización satelital y otros mecanismos para reducir o disuadir los atentados contra los vehículos de transporte de mercancía.
- Establecer sistemas de comunicación con choferes en ruta, que permitan monitorear la ubicación de forma periódica.
- Generar sistemas de claves o alertas en caso de incidentes sospechosos en carretera.
- Seguridad Informática. La seguridad de los sistemas es cada vez más importante ya que muchos fraudes pueden ser perpetrados desde la red (interna o externamente). Asesorarse e implementar ciertas acciones mínimas como la adquisición de un buen firewall, antivirus o políticas sobre el uso de los sistemas, como cambios de contraseñas y respaldos de la información.
- Dispositivos y sistemas automatizados de vigilancia como: CCTV, dispositivos de alerta, botones de pánico, luces de emergencia, etc.
- Pólizas de seguro. especialmente si la actividad de la empresa es de alto riesgo o está ubicado en zonas de alto riesgo.

- Reforzar la seguridad de las instalaciones. Un análisis de riesgo significa determinar los puntos vulnerables por donde un delincuente podría intentar entrar, para reforzar puertas y ventanas o cerraduras más seguras.
- Adecuada iluminación. La cantidad de luz adecuada a las instalaciones y operaciones es muy útil para alejar a los intrusos, y mejora la visibilidad.
- Revise periódicamente los basureros, bodegas, rincones, establezca medidas de seguridad adicionales en los sitios de manejo de basura, y de reciclaje.
- Rotulación visible de las áreas críticas y barreras físicas adecuadas al entorno, que impidan el acceso a personas no autorizadas.
- Controle y revise regularmente que las puertas que no utilice se mantengan cerradas con llave o con candados.
- Evite obstáculos que puedan bloquear la visibilidad en ventanas o en mallas perimetrales o que permitan escalonamientos.
- Desarrolle un sistema de comunicación y apoyo mutuo con autoridades.
- Establecer y mantener un eficiente sistema de gestión de riesgos en cada proceso.
- Mantenga un registro actualizado de los activos e inventarios y revíselo periódicamente.
- Verifique con regularidad si los dispositivos de seguridad están funcionando correctamente.
- Establecer procedimientos de control de llaves y combinaciones de cerraduras.
- Áreas de estacionamiento; carga o descarga de materias primas o producto terminado deben estar alejadas del edificio principal.
- Asegúrese que sus empleados tengan un lugar seguro en donde dejar sus posesiones (bolsos, y abrigos) durante las horas de trabajo y que las mismas estén controladas.
- No establezca una hora o ruta habitual, cuando haga depósitos bancarios o transacciones en efectivo.
- No discuta cuestiones confidenciales frente a extraños o en sitios no adecuados, ya que podría estar brindando información valiosa.
- Realizar rondas periódicas en las instalaciones para identificar personas o actividades sospechosas.

Qué hacer si se es víctima de robo, hurto o asalto?

Es importante que lo comunique lo antes posible a su superior inmediato o Encargado de Seguridad, seguir procedimiento establecido por la política que rige el sistema de denuncia de actividades sospechosas de su empresa, si sospecha que esto pudiera pasar en el futuro o si cree ser víctima de otra forma de actividad ilegal.

- Mantenga la calma, evite defenderse o reaccionar violentamente contra asaltantes o ladrones, esto podría provocar consecuencias más graves contra su integridad física o la de otras personas.
- Aviso inmediato a la persona encargada y/o responsable de la seguridad.

- Dar aviso a las autoridades correspondientes.
- Asegurar y prohibir el acceso a la zona debidamente aislada y/o delimitada, con el fin de proteger la escena del hecho.
- Elaborar un acta con la situación acontecida, incluyendo detalles del lugar donde ocurrió el suceso. Incluir videos y/o fotografías.
- Levantar una lista con el nombre de todas las personas presentes en el sitio durante el evento.
- Presenciar la llegada de las autoridades, y anotar en una bitácora la situación detectada.
- Esperar recomendaciones de las autoridades.
- Realizar el informe de lo acontecido, y presentar denuncia formal ante la autoridad competente.
- Colaboración con las autoridades en la etapa de recolección de pruebas y la investigación del caso.
- Indíquele a la policía todos los objetos que los sospechosos hayan dañado o robado o bien que se hayan dejado en el sitio.
- Promueva y lleve a cabo una política para denunciar a los delincuentes. Desarrolle y haga cumplir una política para denunciar estas actividades delictivas.
- Evalué la situación y refuerce sus medidas de seguridad en general,
- Hacer una reevaluación de las medidas preventivas establecidas en la gestión de los riesgos.

Un asalto o toma de rehenes es una situación crítica. Cualquier circunstancia puede desencadenar una tragedia, por lo tanto, lo más seguro es que esta situación crítica dure lo menos posible. Dicho de otra forma, cuanto más rápido se vaya el delincuente, más rápido se estará a salvo.

- Ante todo; mantenga la calma. Evite defenderse o reaccionar violentamente contra asaltantes o ladrones.
- No oponga resistencia, menos aún si los delincuentes portan armas.
- Trate de memorizar lo que escucha y observa, de manera discreta.
- Nunca vea a los asaltantes a los ojos.
- Si los delincuentes escapan en un vehículo memorice y anote el número de placas, el modelo, el color y la marca.
- Si lo toman como rehén, no se resista, ni trate de escapar.
- No toque ningún objeto que haya sido tocado por los asaltantes.
- En caso de disparos tírese al suelo y cúbrase la cabeza.
- Por ningún motivo persiga a los asaltantes.
- Observe detalles que posteriormente pueda facilitar a las autoridades.
- No altere la escena, ni mueva artículos que estén en el lugar de los hechos.