

## 1 OBJETIVO DEL PROCEDIMIENTO

Dar a conocer a cada uno de los clientes internos y externos de Securtronic Ltda. Las medidas mínimas de seguridad, indispensables para prevenir, minimizar y contrarrestar cualquier riesgo de seguridad, que pudiese atentar contra la tranquilidad y desarrollo de las funciones propias de la empresa y la Información de nuestros clientes.

## 2 ALCANCE

Desde la identificación de riesgos y amenazas hasta la implementación y control por parte de cada integrante de la organización.

## 3 DEFINICIONES

**SEGURIDAD:** Es un estado de confianza y tranquilidad, el cual se caracteriza por la garantía de que las amenazas y peligros son o serán contrarrestados mediante la aplicación de medidas oportunas y adecuadas. Constituye un estado de paz y sosiego, adquirido una vez los asociados consideren que están exentos de riesgos, al aplicar las medidas de seguridad necesarias.

**SEGURIDAD INFORMÁTICA:** La Seguridad Informática se refiere a las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad.

**RIESGO DE SEGURIDAD:** Son todos aquellos medios naturales, artificiales evidentes o encubiertos que ponen en peligro la seguridad.

**RIESGOS NATURALES:** Son todos aquellos medios naturales, que por la fuerza misma de la naturaleza causan daños, terremotos, maremotos, inundaciones, incendios, etc.

**RIESGOS PRODUCIDOS POR EL HOMBRE:** Se clasifican en.

**EVIDENTES:** son todas aquellas acciones realizadas de forma manifiesta y sostenible: disturbios, manifestaciones, raptos, secuestros.

**ENCUBIERTOS:** son todas aquellas que se desarrollan sin que nos podamos dar cuenta: sabotajes, espionajes.

**INCENDIO:** es el producto de una reacción química conocida con el nombre de combustión, la cual se da cuando se ponen en contacto tres elementos (material combustible, calor y oxígeno).

**EXPLOSIVO:** Cualquier compuesto químico o mezcla mecánica, que bajo la influencia de una llama o chispa, ocurre un cambio químico repentino al librarse.

**EXTORSIÓN:** es un delito que consiste en obligar a una persona, a través de la utilización de violencia o intimidación, a realizar u omitir un acto o negocio jurídico con ánimo de lucro y con la intención de producir un perjuicio.

## 4 DESARROLLO

### 4.1 Políticas de Seguridad.

- Todo el personal de la compañía debe estar dispuesto, en el momento que sea requerido, a que se realice inspección de seguridad a sus puestos de trabajo, sitios de almacenaje de información e insumos de trabajo.
- Poner en práctica medidas de autocuidado, tanto en objetos personales como en su integridad.

- Proteger la información de la organización, clientes internos y clientes externos.
- Realizar los cambios de claves según la programación del área de sistemas de información.
- Quien incurra en el incumplimiento de este procedimiento estará sometido a sanciones disciplinarias establecidas por la empresa, que pueden ir desde llamados de atención hasta la terminación del contrato.
- Abstenerse de hacer comentarios y divulgar información que comprometa la seguridad de la empresa, los empleados y clientes.
- Abstenerse de ingresar a las instalaciones una vez haya salido de su horario laboral.
- Todo personal externo de la organización debe ser registrado en recepción y debe ser recibido por la persona que lo atenderá, igualmente al momento de retirarse de las instalaciones.
- Ningún vendedor debe ingresar a la empresa en horarios laborales y de descanso.
- Los menores de edad que ingresen a la organización, son de absoluta responsabilidad del adulto que los lleve tanto en la seguridad física del menor, como de los daños que pueda ocasionar a los bienes de la empresa.
- La persona de servicios generales no debe realizar diligencias personales a los empleados de la organización en su horario laboral.
- Al cumplir la jornada laboral y en periodos de descanso, es responsabilidad de todos los empleados dejar debidamente cerradas las puertas, ventanas, grifos de los baños y lavamanos y demás fuentes de agua; además deben dejar apagados los aires acondicionados y las luces de oficinas; y desconectar los equipos electrónicos y zonas comunes de la organización.

- Reportar a las entidades de seguridad de la empresa y a las entidades del gobierno cualquier actividad sospechosa dentro y fuera de la empresa.
- En caso de ocurrencia se debe reportar los hechos a la central de monitoreo vía telefónica a la extensión 772, con la siguiente información, que pasó, como ocurrió, donde ocurrió, personas o área de la empresa afectadas y luego enviar toda esta información por escrito a través de correo electrónico [seguridad@securtronic.com](mailto:seguridad@securtronic.com).
- Cumplir con todos los controles y recomendaciones establecidas en el procedimiento de seguridad y matriz de seguridad de la organización.

## **4.2 Selección Adecuada del Personal.**

El área de Gestión humana es la responsable de contratar personal idóneo de acuerdo a los perfiles que requiere la empresa.

- Verificación de antecedentes y anotaciones públicas.
- Validación y verificación de los datos anexados en la hoja de vida (autenticidad de diplomas, referencias laborales y personales).
- Prueba Psicotecnias.
- Pruebas de sustancias Psicoactivas.
- Entrevista de selección.
- Pruebas de poligrafía.
- Visitas domiciliaria.
- Examen médico.

## **4.3 Desvinculación de personal.**

El área de Gestión Humana y Sistemas, son los responsables principales de tramitar la desvinculación de los trabajadores.

- Gestión Humana solicita al área de sistemas el Backup de la información antes de la notificación del empleado que no prestará más los servicios en la organización.
- Entregar los elementos que lo identifican como empleado de Securtronic y demás elementos que le fueron entregados para el cumplimiento de sus funciones.
- Notificación a clientes Internos y externos de la desvinculación de los empleados de los cargos críticos a nivel nacional.
- Entrega de formato de paz y salvo, con las firmas que garantizan la entrega correcta y completa del cargo.
- En caso de periodo de vacaciones, el área de Gestión Humana y Gerencia administrativa, define quién hace el remplazo y contingencia para cada cargo.

#### **4.4 Verificación de datos de clientes.**

Los procesos de Comercial y Compras, son las directas responsables que todos los clientes y proveedores cumplan con los siguientes requisitos.

- Verificar en las centrales de riesgos, a los clientes externos y proveedores con previa autorización, a través de tratamiento de datos.
- Verificar en: Listas Clinton, Contraloría, Procuraduría y Policía Nacional a clientes externos y proveedores.
- Análisis de seguridad a los clientes externos.
- Actualización Cámara de Comercio y visitas de inspección a proveedores.

- Verificar la legalidad de sus ingresos, dejando como evidencias los registros de. Notificación recomendación y validación análisis de gestión de seguridad y riesgos y demás establecidos en cada proceso.

## **4.5 Control de Entradas y Salidas de Securtronic.**

Todos los trabajadores de la empresa deben cumplir con el protocolo de entradas y salidas sin excepción alguna.

- En la entrada principal de la sede de Medellin se cuenta con un sistema de ingreso por medio de video portero IP, el cual permite a la recepcionista visualizar la persona que solicita el ingreso, la persona debe anunciarse y solicitar autorización para ingresar, una vez la recepcionista valide la información con el empleado, procede abrir la puerta y posteriormente a ingresarlo en el software de registro.
- La Central de Monitoreo cuenta con visualización y mecanismo de apertura como contingencia a la recepción.
- La entrada principal cuenta con dos puertas controladas con electroimán.
- La primera apertura de ingreso a los empleados se realiza desde la Central, previa visualización con las cámaras. Si no se cuenta con la autorización de la seguridad, no se puede abrir las instalaciones antes de las 06:00 am a ningún empleado diferente al personal operativo de la Central.
- La recepcionista labora hasta las 17:15 con el fin de controlar la salida de los empleados, en caso de que una persona requiera salir después de la jornada laboral, debe abrir las puertas manualmente de forma independiente, abriendo primero la reja externa, siempre asegurándose que las dos puertas queden totalmente cerradas, quedando bajo su responsabilidad el cierre de éstas.

- Todos los paquetes, sobres y facturas que llegan a la empresa dentro del horario laboral, deben ser verificados por la recepcionista, la mercancía de almacén la verifica directamente el almacenista.
- No se permite recibir ningún domicilio, paquete, sobre, mercancía, en horario diferente al laboral establecido en la empresa que es de (lunes a viernes de 7am a 12 am y de 1 pm. A 5 pm. En caso de una eventualidad se debe coordinar con el responsable de seguridad.
- No se permite el ingreso a las instalaciones del personal interno o externo con casco o cualquier accesorio que impida el reconocimiento facial del individuo.
- El control de ingreso y salida de bienes y equipos de la empresa debe hacerse con la debida autorización del jefe inmediato y con notificación a la Gerencia administrativa. Se debe dejar registro en la planilla y se debe hacer verificación de lo existente. Cualquier equipo que salga de las instalaciones debe ser registrado en la planilla de control.
- En horario no laboral, ningún empleado puede abrir o permitir el ingreso a las instalaciones ya sea del personal interno o externo a la compañía. Se hace énfasis en el horario laboral de 7 a 12 y de 13 a 17 de lunes de a viernes.
- No se permite el ingreso de personas que comercialicen algún objeto diferente a los servicios inherentes a la empresa, cualquier proveedor que visite las instalaciones debe avisar con anterioridad y debe estar coordinado por el empleado del proceso.
- En la ciudad de Cartagena el control del ingreso de todo el personal externo a las instalaciones se realiza de lunes a viernes, en horario laboral, a través de la recepcionista.

- El personal administrativo utiliza el control de acceso para el ingreso en horario laboral; el control de ingresos en horario no laboral se realiza con el vigilante de Segurcol, previa autorización de la Coordinadora Administrativa Costa y / o Jefe Inmediato.
- El personal interno. Debe portar siempre el carnet de identificación de Segurtronic Ltda. de manera visible, de tal manera que permita ser identificado en el acceso principal y en las instalaciones.
- Notificar el ingreso de equipos personales si es el caso, el cual debe quedar documentado en el formato registro de ingreso y salidas de equipos y al retirarse, debe registrar su salida.
- Personal Externo: antes del ingreso en la recepción éste debe ser autorizado por el funcionario que atenderá la visita. La recepcionista debe dejar registro en el formato registro de ingreso y salidas de personal externo indicando la fecha y hora de ingreso, nombre, número cédula, persona que autoriza, fecha y hora de salida. El visitante debe dejar un documento de identificación con foto mientras permanece en la empresa, a cambio se le entregará una escarapela con identificación de visitante. El área que atienda la visita debe salir a la recepción y dirigirlo al destino final, al igual que la salida. La espera del visitante siempre debe hacerse en la recepción, nunca puede acceder a las instalaciones sin el acompañamiento del empleado.
- Se debe entregar al personal externo una escarapela de visitante que lo identificara dentro de la Organización.



## 4.6 Control de Acceso.

Es responsabilidad de todo el Personal de la Empresa y Gestión Humana darle cumplimiento al procedimiento de seguridad físico y electrónico.

- Todo el personal interno que ingrese a las instalaciones deberá marcar sin excepción su entrada con tarjeta o huella digital según corresponda, en caso de pérdida u olvido, se debe reportar a la recepción y este a su vez a Gestión Humana, con el fin de dejar documentado y llevar un registro del empleado para tomar los controles respectivos.

**Nota.** La asignación de una nueva tarjeta de control de acceso tiene un costo de diez (10.000) mil pesos.

En caso de pérdida o robo del carnet de la empresa se debe realizar una denuncia ante inspección de Policía o Fiscalía y traer registro al área de Gestión Humana.

## 4.7 Demarcación de zonas críticas.

La Gerencia Operaciones y/o Sistemas, como responsables de seguridad deben realizar las siguientes actividades

- Identificación de zonas críticas.
- Señalizar las zonas identificadas como restringidas.
- Definir controles de seguridad.

## 4.8 Horario de Trabajo.

El horario laboral del personal está definido de la siguiente manera:

**4.8.1 Personal de Planta.** Labora de 07:00am a 12:00pm y de 1:00pm a 5:00 pm de lunes a viernes.

**4.8.2 Cuando se requiera salir después de la jornada laboral.** Se debe reportar al correo seguridad@segurtronic.com, centralmedellin@segurtronic.com, saludocupacional@segurtronic.com y tomar todas las medidas de seguridad, siempre verificando que los equipos y luces queden apagados, puertas y ventanas bien cerradas, y dejando la oficina siempre con seguro.

**4.8.3 Personal técnico.** Labora de lunes a viernes de 8:00am 12:00m y 2:00pm a 6:00 pm, sábado de 8:00am a 12:00m.

**4.8.4 Operadores.** Laboran de 6:00am a 6:00pm y de 6:00pm a 6:00am de lunes a domingo.

**4.8.5 Cuando se requiera el ingreso a las instalaciones.** De lunes a viernes con un margen mayor de una hora al horario establecido, se debe informar con anticipación al área de Seguridad de la compañía mediante correo electrónico a la dirección seguridad@segurtronic.com.

## 4.9 Ingresos fines de semana y horario no laboral.

**4.9.1 Personal Interno.** cuando se requiera ingresar a la empresa en horas no laborales se debe solicitar previa autorización del jefe inmediato; en Cartagena, la Coordinación Administrativa y el jefe inmediato serán quienes se encargarán de

dar el visto bueno y notificar al área de Seguridad (correo como soporte) seguridad@securtronic.com (Zona Centro).

[seguridad@securtronic.com](mailto:seguridad@securtronic.com) (Costa). Todas estos permisos y autorizaciones deben hacerse antes de las 4 de la tarde el día viernes, y se seguirá el mismo procedimiento de entrada, mostrando el carnet y utilizando el control de acceso necesario para el ingreso; si no se cumple con lo anterior no se permitirá el ingreso, excepto a la Gerencia General y al Gerente de Operaciones, al Sistemas.

**4.9.2 Personal Externo:** cuando se requiera el ingreso de personal externo a realizar trabajos, debe ser con previa autorización de la Gerencia Administrativa, quien se encargará de dar el visto bueno y notificar a las áreas de Seguridad, Seguridad y salud en el Trabajo a los correos seguridad@securtronic.com, saludocupacional@securtronic.com; esto debe ser informado con una día de anterioridad, relacionando la empresa, nombres, número de identificación, labores a realizar, área de intervención y horario de permanencia en la empresa, todo con previa validación de la información personal.

**4.9.3 Quienes deben Autorizar.** El Gerencia Operaciones, La Gerencia Administrativa y Gerencia General para la zona centro, para la zona Norte se realiza con la Coordinación Administrativa y o Gerencia de Operaciones, se deben comunicar con la Central de Monitoreo y darán las indicaciones para el ingreso. Una vez tramitado el ingreso se debe validar la desactivación de la alarma teniendo acceso únicamente al área donde se va a laborar.

## **4.10 Ingresos después de la salida.**

Si después haber registrado la salida de finalización de la jornada laboral, algún empleado requiere ingresar nuevamente a las instalaciones, debe hacer el mismo procedimiento de autorización de horario no laboral.

Siempre se debe marcar la salida en el control de acceso, cuando se requiera el retiro de algún equipo, debe dejar registro en la planilla de control de equipos. El empleado debe asumir cualquier pérdida o daño del mismo.

## **4.11 Uso de parqueadero y zona externa.**

Los vehículos que quedan en la zona externa son de responsabilidad de cada empleado, deben implementar medidas de autoprotección con los elementos tales como: candados, seguros, alarmas y cualquier dispositivo que impida la sustracción; así mismo son responsables de la ubicación del vehículo ante las autoridades de Tránsito.

## **4.12 Manejo de sistema de alarma.**

Se cuenta con un panel de alarma 18- 64, particionado de la siguiente manera:

**Partición 1:** primer piso área común, entrada principal, recepción y comercial.

**Partición 2:** Almacén y Bodega Seguridad y Salud en el Trabajo.

**Partición 3:** Coordinación servicios y área técnica.

**Partición 4:** Gestión Documental.

**Partición 5:** Contabilidad.

**Partición 6:** Cartera.

**Partición 7:** Sala de juntas 2do piso, Facturación y CRM.

Partición 8: pasillo y patio del segundo piso.

### **4.13 En el tercer piso se encuentra con un panel 1832 con una partición.**

Zona común 3 pisos y pasillos.

Gerencia General, Revisoría Fiscal, Contabilidad

Oficina de Sistemas.

### **4.14 Personal responsable del sistema de alarma dentro de la organización.**

#### **Medellín.**

Alarma primer y segundo piso.

Partición 1: Operadores.

Partición 2: Almacenista y Coordinación SST.

Partición 3: compras e Implementación.

Partición 4: Coordinación Archivo y correspondencia.

Partición 5: Proyectos.

Partición 6: Dirección de Cartera.

Partición 7: CRM y Facturación.

Partición 8: Operadores.

Alarma tercer piso.

Contabilidad

#### **Cartagena.**

Partición 1: Administración y cartera

Las demás sucursales según directrices administrativas:

Las personas anteriormente asignadas son las directas responsables de la seguridad de cada área, del cerramiento de puertas y ventanas de cada oficina; de armar y desarmar el sistema de alarma, así mismo, del manejo y/o entrega de la clave a otro funcionario.

## **4.15 Control de llaves.**

Los operadores, Gerencia de Operaciones y Asistente Monitoreo son responsables de:

- llevar el formato registro de préstamo de llaves, con fecha, hora entrega y devolución.
- El préstamo de llaves se hará exclusivamente si el funcionario extravió la original; para que se haga el efectivo el préstamo debe solicitar el permiso a la Gerencia Administrativa o Gerencia General para la entrega del duplicado que reposa en la Central, esta solicitud debe enviarse por escrito con la debida autorización al correo de seguridad@securtronic.com para autorizar la entrega.
- En caso de pérdida, el empleado asumirá el costo del duplicado; si el duplicado también sufre algún inconveniente, el empleado asumirá el costo del cambio de cerradura.
- Zona costa, el control lo realiza la Coordinación Administrativa.
- Se firma la planilla de control de préstamo de llaves en el momento de entrega de las llaves a cada responsable y se hace un seguimiento a los préstamos.
- En caso de pérdida de las llaves, el empleado debe hacerse responsable de los gastos que genera el duplicado.

## **4.16 Manejo de la información de la organización, clientes internos, externos y proveedores.**

- Existe un contrato de confidencialidad con cada uno de los empleados para garantizar la protección de información.
- Equipos de cómputo: la información corporativa debe residir en las bases de datos de los servidores, si por alguna razón esto no es posible y su manejo se realiza de forma local, el usuario debe documentar los desarrollos realizados.
- Memoria USB: toda información contenida en los recursos informáticos de SEGURTRONIC LTDA. Es propiedad de la compañía y esta se reserva sus diferentes usos. Además, se considera confidencial y queda prohibida su utilización con fines ajenos a lo laboral.

## **4.15. Circuito Cerrado de TV.**

- Se instala un sistema de cámaras ubicadas estratégicamente en la empresa, las cuales tienen un periodo de grabación por movimiento, esta se almacena en un sistema de cola.
- Los registros y grabaciones son confidenciales y en caso que se requieran deben ser autorizadas por Gerencia General, Gerencia Administrativa o entes de control, que dará las instrucciones para la disposición final.
- De acuerdo a las directrices de la Gerencia General o Gerencia Administrativa se procede al almacenamiento y/o conservación de estos archivos.

## **4.17 Administración de llamadas telefónicas.**

- Se cuenta con una planta telefónica que permite la interacción entre las sedes y a su vez, tener el registro de llamadas entrantes y salientes.

- Las grabaciones de llamadas de la Central de Monitoreo son almacenadas en un PC por 2 mes, las cuales se utilizan cuando requieren algún tipo de información.
- Contactos de Emergencia.
- Correos electrónicos.
- [seguridad@segurtronic.com](mailto:seguridad@segurtronic.com)
- [gerenciaoperaciones@segurtronic.com](mailto:gerenciaoperaciones@segurtronic.com) cel. 313-5343171.
- [sistemas@segurtronic.com](mailto:sistemas@segurtronic.com) cel. 350-3433039
- [gerenciageneral@segurtronic.com](mailto:gerenciageneral@segurtronic.com) cel.313-6725945
- Central de Monitoreo. [centralmedellin@segurtronic.com](mailto:centralmedellin@segurtronic.com)
- Teléfonos- 4120078- 4033513 Celulares 312-6199016- 312-6218595- 313-5861794—312-6917181
- [saludocupacional@segurtronic.com](mailto:saludocupacional@segurtronic.com) 444.19.26 ext. 744. 312.6198996
- Coordinador de emergencias – [auxiliarcontable4@segurtronic.com](mailto:auxiliarcontable4@segurtronic.com) 444.19.26 ext. 789.
- Bomberos. 1.2.3.
- Policía Nacional. Cuadrante Floresta. 300-6946226 - 300 561.19.63
- CAI Más Cercano: Santa Lucia. 4211912.
- Estación Laureles 4131454.
- Clínica salud Coop de la 80 – Teléfonos: 460.00.03- 460.00.05
- Clínica las Américas Tel. 341.29.46.
- Clínica Medellin centro Tel.356.85.85.
- CES centro Tel.6.576.72.72.
- San Vicente de paúl 448.26.26

## **4.18 Requisición de usuario y equipo de cómputo.**



- Gestión Humana realiza la solicitud al área de sistemas de usuario de red y equipo de cómputo con la información del puesto de trabajo y sus recursos asignados.
- Se crea espacio en la red para almacén la información con respecto al cargo.

#### **4.19 Administradores de la información.**

Es responsabilidad del área Sistemas de la organización:

- Tener para todos los usuarios un espacio en el servidor para salvaguardar la información.
- Backup en cinta encriptado con una disposición final desconocida.

#### **4.20 Manejo de la información.**

- Capacitar al personal sobre la importancia de salvaguardar la información en la carpeta del servidor
- Verificar la información que se guarda en el servidor por cada uno de los usuarios.

#### **4.21 acceso a la información.**

- Se clasifican según sus funciones y directrices de Gestión Humana y Gerencia General.
- Se asignan los permisos.
- Se hace una revisión de activos e inactivos.

#### **4.22 Copias de seguridad.**

- Se hace a través de las carpetas del servidor.
- Revisión de las carpetas en los servidores.
- Backup en cinta magnética diariamente y un acumulado mensual.

- Se guarda en un lugar de seguridad externa a la empresa.

#### **4.23 Planes de contingencia.**

- Realizar, implementar y garantizar los planes de contingencia para los sistemas informáticos de la compañía.

#### **4.24 Instalación de software.**

- Verificar la necesidad del SOFTWARE.
- Mantener la restricción de los usuarios para la instalación.
- Instalar de acuerdo a la necesidad del usuario.

#### **4.25 Control y seguimiento al procedimiento.**

- Calcular indicadores que permitan hacer análisis de resultados e implementar acciones según sea el caso.

#### **4.26 Mantenimiento de Infraestructura.**

- La Gerencia Administrativa establece el cronograma de mantenimiento de Infraestructura, que incluya puertas, cerraduras, techos, griferías, paredes, pisos, sistema eléctrico, cableado estructurado, aires acondicionados, equipos y herramientas, extintores, sillas, iluminación.

#### **4.27 Mejora continua.**

Implementar mejoras de acuerdo al resultado de indicadores e informes de auditorías Internas y Externas.

## **5 ANEXO.**

Paz y Salvo.

Planilla control de entradas y salidas equipos.

Registro de préstamo de llaves.

## 6 CONTROL DE CAMBIOS.

FECHA DE LA MODIFICACIÓN	VR	MOTIVO DE LA MODIFICACIÓN	DESCRIPCIÓN DEL CAMBIO
15-Ene-2017	1	Migración del Documento y ajustes	Con la integración de las empresas del Grupo Record, se crea un documento donde se describe la forma como se debe realizar la nueva documentación del SGI. Teniendo en cuenta los cambios de Iso 9001 versión 2015.
30-Ene-2019	1	Actualización	Se ajustan las actividades de acuerdo a los cambios administrativos y acciones de los procesos.

\_\_\_\_\_ **Fin del Documento** \_\_\_\_\_