

	Política de Seguridad de Fruno			Rev. B	Pag.1 (22)
Elaborado por:	Fecha	Código	Tipo de Documento	Departamentos	
Jonathan Espinoza	04/10/2024	FR-PO-SE01	Interno	Seguridad	
Revisión 1 por:	Revisión 2 por:		Aprobado por:		
Mauren Vega	Andrea Pineda		Jonathan Espinoza		

Política de Seguridad de Fruno

1. Objetivo.

Establecer e informar los lineamientos que permitan a la empresa mantener un ambiente seguro y ordenado, para el resguardo de la integridad de los bienes y activos, así como la de sus colaboradores y de sus clientes.

2. Alcance.

La política de seguridad se extiende y deberá ser acatada por todo el personal de Fruno que se encuentre en las instalaciones de la compañía, así como en sus filiales, el personal de seguridad (guardas de seguridad) y clientes, visitantes y proveedores que hagan uso de las instalaciones de la empresa.

3. Responsables.

- **Oficial de seguridad o jefe de seguridad:** es responsable de mantener un nivel adecuado de seguridad y conforme con los requisitos establecidos por la empresa para la realización de sus operaciones y las de los clientes a los que la empresa presta servicios, así como de realizar reportes de seguridad en los casos en donde se evidencie un incumplimiento a esta u otras políticas generales dentro de la organización, notificando a RRHH o a las jefaturas según sea el caso.
- **Oficial de seguridad de TI o jefe de seguridad de TI:** es responsable de mantener un nivel adecuado de seguridad y conforme con los requisitos de seguridad a niveles lógicos y de la red, adecuados para la realización de las operaciones de la empresa y de los clientes a los que la empresa presta servicios, así como de asignar los accesos correspondientes al personal, para el ingreso a la empresa, y a los sistemas que se encuentren bajo su jurisdicción.

- **Guarda de seguridad:** es responsable de velar por el cumplimiento de los puntos que se indican en este documento, así como los procedimientos pertinentes del puesto. Además, debe realizar reportes al jefe de seguridad según corresponda.
- **Departamento de recursos humanos (RRHH):** es responsable de recibir y atender los reportes realizados por seguridad, con el fin de aplicar las sanciones disciplinarias cuando se presenten incumplimientos. Además, es el responsable de comunicar a todo el personal las políticas de la empresa mediante los canales oficiales de comunicación, y de las secciones puntuales en donde se mencione a RRHH en esta política.
- **Personal, colaboradores:** es responsable de acatar, cumplir y seguir con los lineamientos indicados en esta política, garantizando un ambiente de trabajo seguro.
- **Visitante, clientes y proveedores:** es responsable de acatar las indicaciones de seguridad asignadas ya sea por el jefe de seguridad, el guarda de seguridad, o el contacto de la empresa a quien visita o provee un servicio, durante la visita, permanencia y uso de las instalaciones de la empresa.
- **Jefaturas:** son responsables de velar porque el personal acate y cumpla con esta política, además de realizar sanciones en conjunto con RRHH y de mantener un listado actualizado de su personal a cargo en el sistema de marcas de la empresa.

4. Documentos aplicables.

- FR-PO-SE02 Política de revisión del personal
- FR-PR-SE02 Entrega de gafetes desde seguridad
- FR-PR-SE13. Ingreso de dispositivos de colaboradores para reparación
- FR-PR-SE16. Procedimiento. Notificación de visitas
- FR-PO-TI01. Política de Seguridad de las Tecnologías de Información y Comunicación
- FR-PO-TI02. Política de gestión de usuarios y contraseñas

- FR-PO-RH01. Reclutamiento y Selección.
- FR-PO-RH03. Relación entre Colaboradores y Clientes
- FR-PO-RH07. Código de vestimenta.
- FR-PO-RH10. Política de Uso del Gafete.
- FR-PR-RH03. Procedimiento de Salida del Personal
- FR-PO-CO02. Política de activos fijos.

5. Definiciones.

Oficial de seguridad o jefe de seguridad: es la persona que labora para la empresa y que está en una posición jerárquica próxima del nivel de gerencia general de la empresa cuya misión es la redacción, implementación, auditorías, control y actualización de políticas de seguridad.

Oficial de seguridad de TI o jefe de seguridad de TI: es la persona que labora para la empresa y que está en una posición jerárquica próxima del nivel de gerencia general de la empresa cuya misión es la redacción, implementación, auditorías, control y actualización de políticas de seguridad de índole informático.

Guarda de seguridad: es la persona contratada por la empresa para ejercer funciones de vigilancia, monitoreo, reportes y revisión del personal.

Visitante - Cliente: toda persona externa a la empresa que se apersona al edificio por motivos laborales o comerciales.

Proveedores: toda persona que provee o abastece a la empresa de lo necesario o conveniente para un fin determinado.

Política: Son el conjunto de normas internas que se diseñan para regular y delimitar las reglas de conducta dentro de una organización.

Filiales: tiendas, quioscos administrados por personal de Fruno.

Repuestos sensibles: son los repuestos que representan un valor económico alto o bien repuestos que por su estructura almacenan información confidencial o de seguridad.

Áreas operativas: son las siguientes áreas: Taller Samsung, Taller Otras Marcas, Taller Ingenico, bodegas e inventarios, ingreso, despacho, logística.

Áreas administrativas: son las siguientes áreas: proyectos, servicios regionales, contabilidad, homologaciones, contact center, cumplimiento y comercial.

IMEI (International Mobile Station Equipment Identity, en inglés): es un código de 15 dígitos pregrabado por el fabricante para identificar cada equipo móvil (celular).

6. Desarrollo.

Política.

6.1. Todos los colaboradores deben respetar y acatar las instrucciones de seguridad, así como respetar al personal de seguridad designado.

6.2. Todos los colaboradores deben respetar y acatar los protocolos definidos por la empresa, según sean notificados por RRHH mediante correo electrónico o bien por las jefaturas.

Oficial de Seguridad – Jefe de Seguridad.

6.3. Las directrices de seguridad que la empresa establece se determinan por medio de gerencia general en conjunto con el oficial de seguridad y son comunicadas al guarda de seguridad, así como a los colaboradores por medio de la distribución de esta política, a través de departamento de recursos humanos mediante correo electrónico a todo el personal y deben ser incluidas en los temas de inducción de todo colaborador.

6.4. El oficial de seguridad y el oficial de seguridad de TI realizarán funciones de concientización sobre la seguridad en la empresa, velando por el manejo seguro de la información y procesos de los clientes con quien Fruno mantiene una relación laboral.

6.5. Cualquier indicación fuera de esta política o de las políticas de la empresa quedan sin validez.

Reclutamiento y selección de personal.

6.6. Fruno por medio del departamento de RRHH, tomará las medidas necesarias para la verificación de los aspirantes, así como de la revisión de hojas de vida, referencias laborales u otros medios que Fruno considere necesarios tales como la solicitud de la hoja de delincuencia del aspirante, la cual y para efectos de Costa Rica es emitida por el poder judicial, esto con el fin único de resguardar tanto la seguridad física como laboral de la empresa.

6.7. La notificación de ingreso de nuevo personal es realizada por medio de correo electrónico por parte de RRHH a las áreas correspondientes. Cualquier otra notificación que no sea realizada por RRHH será una comunicación no oficial.

6.8. Para el ingreso a las instalaciones de Fruno, solamente RRHH podrá asignar el gafete temporal en coordinación con seguridad y solamente RRHH podrá asignar el gafete oficial para cada persona que labora en la empresa.

6.9. Para más información, ver la política *FR-PO-RH01. Reclutamiento y Selección.*

Rotación de personal.

6.10. La rotación de personal quedará a consideración de la gerencia general o bien las jefaturas de la empresa.

6.11. La rotación de personal esta sujeta al comportamiento del negocio y del mercado.

6.12. Para tales efectos, la empresa realiza procesos de selección y de despidos, ambos procesos serán acompañados por sus variantes, ejemplo: asignación de accesos, eliminación de accesos, etc.

6.13. RRHH podrá reservarse el derecho de la información referente a estadísticas de rotación de personal.

Seguridad física.

6.14. La empresa se encuentra ubicada en Río Segundo de Alajuela, Zona Franca Alajuela, Costa Rica. La zona franca cuenta con control de acceso por medio de tarjeta, además de guardas de seguridad, cámaras de vigilancia, portones de ingreso y agujas de control, para acceso de personas y vehículos respectivamente.

6.15. La zona franca coordina por medio de RRHH de Fruno la entrega de una tarjeta de acceso para el ingreso a la zona franca a cada colaborador de la empresa.

6.16. La seguridad de la zona franca es de 24/7.

6.17. La empresa, además dispone de guardas de seguridad durante las horas operativas o jornadas previamente coordinadas.

6.18. Por su seguridad, la empresa cuenta con sistemas de cámaras para grabación de video y de monitoreo CCTV 24/7, además de sistemas de alarma con vigilancia y respuesta armada 24/7.

6.19. En el caso de las alarmas, se realizarán pruebas de funcionamiento al menos una vez al año.

6.20. En el caso de videos, se harán revisiones periódicas o puntuales según sea el caso.

6.21. Todo requerimiento de revisión de videos o de alarmas, debe ser escalado mediante correo electrónico al jefe de seguridad, detallando el requerimiento y el motivo por el cual solicita la revisión de videos.

6.22. Se prohíbe la solicitud de videos de seguridad o de información de seguridad al guarda de seguridad.

6.23. Toda revisión de videos de seguridad será realizada solamente por el guarda de seguridad en coordinación con el jefe de seguridad.

6.24. La empresa dispondrá de guardas de seguridad para cubrir los turnos según la jornada laboral. Los turnos de trabajo podrían variar de acuerdo a disposiciones del jefe de seguridad o de la compañía.

6.25. Es deber del guarda de seguridad seguir responsablemente las indicaciones y procedimientos que la empresa le ha comunicado.

6.26. El jefe de seguridad y de TI son los encargados de dar los accesos para la revisión de videos,

Control de marcas.

6.27. La empresa dispone de un sistema de marcas vía web para registrar los tiempos de entradas, recesos y salidas del personal.

6.28. El personal debe reportar su entrada, recesos y salida de la jornada laboral, en el sistema de marcas desde su computadora de trabajo o estación asignada por su jefatura. En caso de omitir esta acción podrá ser sancionado por RRHH.

6.29. Se deben respetar los horarios de entradas y salidas a la empresa así como los horarios de recesos.

6.30. El enlace para acceder al sistema de marcas es <https://asistencia.nargallo.com/>, donde se visualiza la siguiente información:

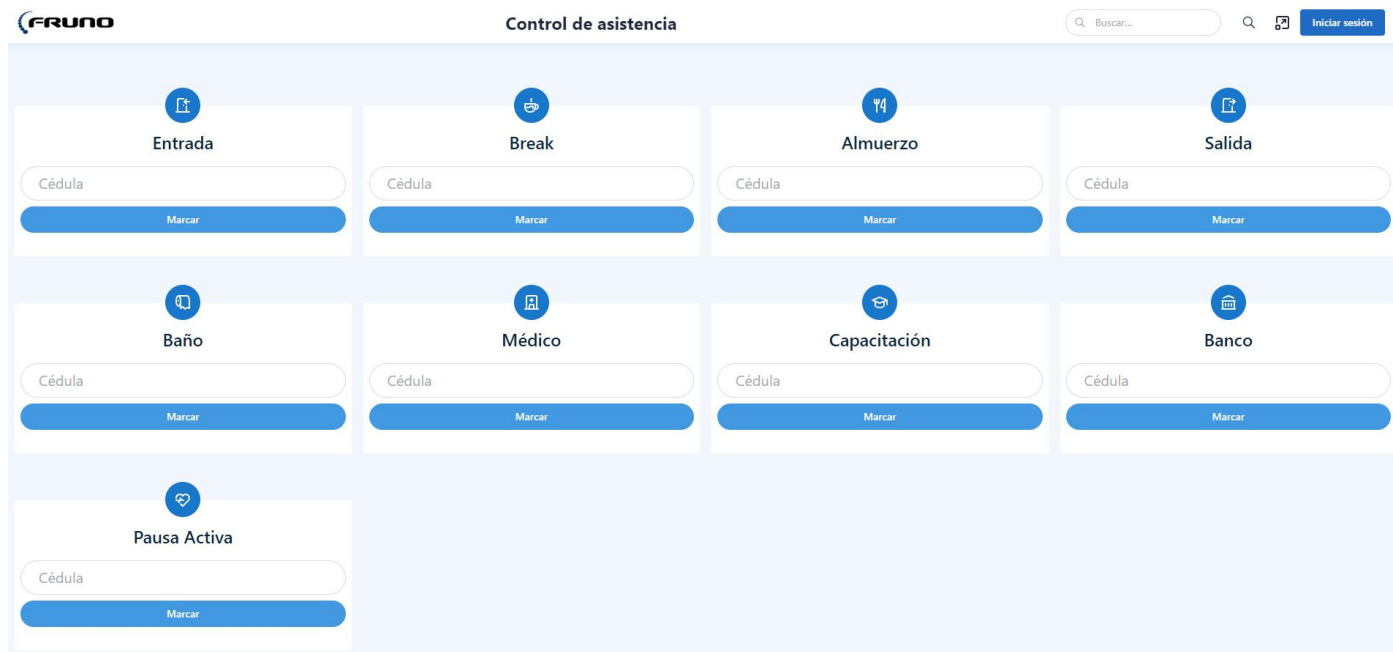


Imagen del sistema de marcas.

6.31. Se debe tener en cuenta que para las marcas: Break, Almuerzo, Baño, Médico y Capacitación se debe realizar dos marcas, la primera marca será como salida del puesto, y la segunda marca será como ingreso o retorno al puesto.

6.32. RRHH está autorizado a gestionar y comunicar los reportes de marcas de todo el personal, este reporte es enviado por correo electrónico en formato de excel a cada jefatura, sin embargo todas las jefaturas tienen acceso a descargar estos reportes directamente de nuestro sistema de control de marcas.

6.33. En caso de cualquier colaborador olvide realizar la marca, debe de enviar un correo a RRHH con copia a su jefatura realizando la notificación del error o el olvido con alguna de sus marcas para que RRHH pueda realizar el ajuste y la anotación.

6.34. La inscripción y actualización de información del personal en este sistema se encuentra a cargo de cada jefatura.

6.35. Todo colaborador que sea nuevo ingreso a la empresa debe reportar a su jefatura los dispositivos electrónicos que trae consigo a las instalaciones. La jefatura correspondiente realiza la inscripción de estos dispositivos en el control de marcas (incluyendo marca de dispositivo, modelo, IMEI y número de serie) para que estos queden registrados.

6.36. En caso de que algún colaborador cuente con un nuevo dispositivo o requiera hacer una actualización de los dispositivos registrados, debe informar inmediatamente a su jefatura para que este realice la gestión correspondiente en el sistema de marcas.

6.37. En el proceso de salida de las instalaciones, el guarda de seguridad podrá verificar información del personal y los dispositivos que tiene registrados, al escanear su gafete en el sistema de control de marcas, cuando este salga por el área de seguridad. En caso de portar un dispositivo que no se encuentre registrado, se realizará la retención del mismo, y se procederá con la investigación correspondiente hasta determinar que no corresponde a ninguna unidad de la cual la empresa tenga jurisdicción.

Accesos físicos.

6.38. El ingreso del personal a la empresa (Fruno en Zona Franca Alajuela) se realiza por el área de seguridad, ubicado por el área del andén. La empresa dispone de una entrada única para todo el personal en esta sección, y para el ingreso cada colaborador debe utilizar la huella dactilar para realizar la apertura de la puerta del área de seguridad o bien por medio del sensor biométrico, estos accesos serán otorgados por parte de la jefatura de TI.

6.39. La administración del control de acceso físico a Fruno, estará bajo la coordinación del departamento de RRHH y de TI.

6.40. Todo el personal de la empresa debe ser identificado en todo momento, para esto, debe usar su gafete en lugar visible para los procesos de ingreso, de salida y durante sus horas laborales. Para más información por favor consultar *FR-PO-RH10. Política de Uso del Gafete*.

6.41. El uso del gafete es personal y no es transferible, por lo que está prohibido prestarlo al personal interno o externo de la compañía.

6.42. El guarda de seguridad debe verificar que el gafete efectivamente sea de la persona que lo porta, caso contrario no se le permitirá el ingreso y será reportado inmediatamente al jefe de seguridad, recursos humanos o en su defecto a gerencia general.

6.43. Para los casos en donde el control de acceso instalado para aperturas de puertas en el área de seguridad (ingreso y salida de colaboradores) se encuentre en mantenimiento, el guarda de seguridad controlará el ingreso por medio de la verificación del gafete del/de la colaborador.

6.44. Si un colaborador no porta el gafete de identificación de la empresa, el guarda de seguridad impedirá el ingreso a las instalaciones, hasta ejecutar el procedimiento *FR-PR-SE02 Entrega de gafetes desde seguridad*, donde se lleva a cabo la firma de la autorización del ingreso, se realiza la aprobación correspondiente y el guarda de seguridad realiza entrega al colaborador un gafete

temporal, mismo que le permitirá el acceso a la compañía durante el horario de oficina. Dicha autorización debe estar firmada y consentida por el supervisor inmediato, o en su defecto alguna de las personas autorizadas. De repetirse esta conducta, RRHH tomará las medidas disciplinarias junto con la jefatura.

6.45. El gafete temporal será portado mientras el colaborador recupera u obtiene el gafete que la empresa le ha asignado como personal, y durante este periodo el colaborador tendrá las mismas responsabilidades para con la empresa en caso de daño, hurto, pérdida o cualquier acto que le deteriore por negligencia.

6.46. Ningún guarda de seguridad de Fruno, se encuentra autorizado a permitir el ingreso a algún colaborador fuera de horario de oficina, o fuera de las áreas no restringidas si no se cuenta con una autorización formal de la empresa que al menos se haya recibido vía correo electrónico a seguridad@fruno.com. Igualmente, no podrá acceder a las instalaciones de la empresa ninguna persona que no cuente con el gafete de la empresa o con la autorización de ingreso temporal.

6.47. Cada vez que una persona sale de la empresa, debe someterse a revisión con el detector de metales por parte del guarda de seguridad. De igual forma, debe mostrar al guarda de seguridad el bolso, maletín, estuche, cartera, cosmetiquera, o cualquier artículo que pueda ser usado para transportar materiales o activos de la empresa. Para más información por favor consultar *FR-PO-SE02 Política de revisión del personal*.

6.48. El guarda de seguridad debe notificar al jefe de seguridad cualquier irregularidad presentada por parte de los colaboradores, que vaya en contra de esta política. Como por ejemplo: no acatar las instrucciones durante la revisión, uso de vocabulario grotesco o soez, faltas de respeto, en caso de la detección de salida de equipo, material o artículos sin autorización.

6.49. En caso en que durante la salida de colaboradores, el personal de seguridad encuentre la salida de objetos artículos no autorizados, procederá con la retención del objeto o artículo y escalará el tema a su jefatura inmediata.

6.50. El jefe de seguridad puede asignar claves de seguridad al personal para el manejo del sistema de alarmas. La misma, debe ser manejada por el personal con absoluta confidencialidad y responsabilidad siguiendo las indicaciones que, para tal caso, la empresa o el jefe de seguridad le ha asignado. Esta asignación de códigos de alarma es solicitada por el jefe de seguridad mediante el sistema de tickets de la empresa al departamento de TI.

6.51. El guarda de seguridad debe dejar cerradas las puertas de las oficinas, revisar que todos los equipos queden debidamente apagados y activar adecuadamente el sistema de alarma. Solamente podrá mantenerse en el edificio después de la jornada laboral del guarda de seguridad, personas en puestos de gerencia, el jefe de seguridad, o personal del departamento de logística que tenga autorización para realizar el cierre, y serán estos encargados de cerrar y activar la alarma con su código correspondiente.

6.52. La empresa no permitirá el ingreso al edificio de personas que presenten síntomas producto de la ingesta de alcohol y sustancias o drogas ilícitas. Es deber del guarda de seguridad frente a sospecha de un caso de estos, denegar el ingreso y reportar la situación a RRHH. Igualmente, el ingreso a las instalaciones de Fruno con alcohol, drogas o sustancias ilícitas no está permitido.

6.53. Se prohíbe el ingreso a la empresa y a sus filiales a cualquier persona (interna o externa a la empresa) que porte: armas de fuego (pistolas, revólveres y rifles), explosivos, productos pirotécnicos, pólvora, o armas punzo cortantes.

6.54. Se prohíbe al personal de Fruno, el ingreso a las instalaciones de la empresa con: lentes oscuros (de sol), máscaras, cascos (de motocicleta, de bicicleta), gorras, gorros, sombreros, o con cualquier accesorio que impida tener una visión clara de la cara de la persona.

6.55. Se prohíbe a los visitantes de Fruno con ubicación en la Zona Franca Alajuela, el ingreso con celulares, cámaras fotográficas, armas de fuego (pistolas, revólveres y rifles), explosivos, productos pirotécnicos, pólvora, o armas punzo cortantes. El visitante deberá ser recibido por un responsable en Fruno quien coordinó la visita, siguiendo el procedimiento de visitas.

6.56. Toda persona que requiera laborar fuera del rango de horario**, debe coordinar con su jefatura directa, RRHH o el jefe de seguridad. Lo anterior bajo la salvedad de que en todo momento se debe contar con la presencia de una jefatura que asuma la responsabilidad de velar por el cumplimiento de las políticas de seguridad del edificio.

***Consulte el horario actual con su jefatura o con RRHH.*

Áreas seguras.

6.57. De acuerdo con requerimientos de los clientes o según sea determinado por la empresa, se dispondrá de áreas seguras en las instalaciones de Fruno, las cuales serán controladas por medio de un control de acceso. Este genera un registro de los/las colaboradores que ingresan a estas áreas. Sólo las personas autorizadas y equipadas ya sea con una contraseña, gafete o tag, podrá ingresar a estas zonas.

6.58. Fruno por medio del jefe de seguridad, y del jefe de seguridad de TI, asignará permisos de acceso físico a los colaboradores que por la naturaleza de su trabajo deban ingresar a áreas seguras o designadas para la realización de un trabajo especial, que haya sido determinando por Fruno o uno de sus clientes. Así mismo, dejará sin acceso físico a todos aquellos colaboradores que no tengan relación directa con el trabajo realizado en las zonas con accesos controlados.

6.59. El acceso a estas zonas no es transferible de un colaborador a otro. Solamente el jefe de seguridad dará el acceso según sea el caso.

6.60. No se permitirá el ingreso de colaboradores que no se encuentren autorizados.

6.61. El jefe de seguridad y de TI tienen acceso y están autorizados a ingresar a las áreas seguras de la empresa.

6.62. El jefe de seguridad y guardas de seguridad, estarán a cargo del monitoreo de las cámaras de seguridad ubicadas en las áreas seguras.

Accesos lógicos.

6.63. El jefe de seguridad de TI, implementará políticas a nivel de TI que garanticen la seguridad de la red, tanto en equipos de computo, como sistemas y servidores.

6.64. Para información relacionada a la política general de TI, por favor consulte la política *FR-PO-TI01 Política de Seguridad de las Tecnologías de Información y Comunicación*.

6.65. La administración de accesos lógicos, perfiles de usuario, inicio de sesiones, y accesos a programas y aplicaciones, esta a cargo del departamento de TI de acuerdo los requerimientos de la jefaturas.

6.66. El departamento de TI junto con las jefaturas correspondientes asignan los permisos y perfiles de acuerdo al puesto que desempeñe cada colaborador.

6.67. Para el caso en que la empresa realice despido a algún colaborador, o el colaborador renuncie a la empresa, la jefatura inmediata a cargo, debe notificar a RRHH y al departamento de TI para que se eliminen de manera inmediata los accesos lógicos a la empresa y a las zonas seguras según sea el caso, así como el dar de baja a cuentas de correo o accesos a sitios de red de la empresa. Además, RRHH debe notificar al guarda de seguridad para que se impida la entrada física a la empresa. Para más información ver el procedimiento *FR-PR-RH03 Procedimiento de Salida del Personal*.

6.68. El jefe de seguridad de TI implementará y velará por el uso de contraseñas robustas con el fin de fortalecer la seguridad a los sistemas, así como solicitudes automáticas de cambio de contraseña al menos cada tres meses, mismo realizará auditorias de vulnerabilidad de red al menos una vez al año, garantizando de esta forma que la conexión a red sea segura ante posibles ataques.

6.69. Para más información sobre la gestión de contraseñas por favor ver *FR-PO-TI02 Política de gestión de usuarios y contraseñas*.

6.70. TI asegurará que los equipos de computo estén operando con un antivirus debidamente actualizado.

6.71. La empresa por medio de TI limitará el acceso a sitios web no autorizados por la empresa o sus clientes.

6.72. El jefe de seguridad de TI, implementará políticas de red para el bloqueo automático de los equipos de computo en cuanto esto se dejen de usar y no hayan sido bloqueados.

6.73. Se solicita a los colaboradores y colaboradoras que al salir de su puesto de trabajo, se asegure que su equipo de computo quede bloqueado, o bien apagado en el caso de que se retire de la jornada laboral.

Activos de la empresa.

6.74. Que prohibido el retirar o sacar activos de la empresa sin el visto bueno por escrito del departamento de contabilidad.

6.75. Cada movimiento de activos debe ser reportada a la persona a cargo de los activos.

6.76. Para más información ver *FR-PO-CO02. Política de activos fijos*.

Seguridad y confidencialidad de la información.

6.77. Cada colaborador de Fruno debe firmar un contrato de trabajo, un contrato de confidencialidad y de uso de datos, con el fin salvaguardar los intereses de la empresa y de sus clientes.

6.78. Se prohíbe compartir, publicar o comentar sobre información de la empresa o de sus clientes en redes sociales.

6.79. Cada colaborador tiene la obligación de mantener en secreto la información que las partes pretenden compartir entre sí y que desean circular públicamente.

6.80. En caso de que haya duda sobre el irrespeto o violación del contrato de confidencialidad o uso de datos, ya sea que se presente una denuncia por parte de un cliente o colaborador de la empresa, la empresa revisará el caso hasta conocer en detalle lo sucedido. La empresa por medio de los canales correspondientes ante estas situaciones, tomará las medidas necesarias.

Servicios.**Reparación de celulares de colaboradores y ventas de artículos: celulares y accesorios.**

6.81. El colaborador que desee traer un celular a reparar, deberá reportarlo con el guarda de seguridad, indicando el IMEI, modelo y marca.

6.82. Se prohíbe el ingreso de celulares para reparación de manera directa a taller. Para más información ver procedimiento *FR-PR-SE13. Ingreso de dispositivos de colaboradores para reparación.*

6.83. Toda venta de accesorios, artículos o celular que la empresa realice al personal debe tener un factura de compra, de no presentar la factura de compra en el área de seguridad al momento de la salida, no se permitirá la salida del artículo.

6.84. El área de seguridad no recibirá artículos de venta, accesorios o celulares productos de la venta o reparación para entregar a terceros o al personal que solicitó la compra o la reparación.

Visitantes, clientes o proveedores.

6.85. Ver procedimiento *FR-PR-SE16. Procedimiento. Notificación de visitas.*

6.86. Todo visitante debe ser anotado en la bitácora de visitas cuyo registro lo lleva el área de seguridad (guardas de seguridad).

6.87. El acceso a las instalaciones de la empresa para, visitantes, pasantes, proveedores, u otros, se permitirá únicamente por medio del gafete que le ha sido asignado a la persona según su horario de trabajo o condición dentro de la empresa. Nota: para los ingresos que se realicen por el área de seguridad de la empresa, el guarda de seguridad deberá verificar que el gafete efectivamente sea de la persona que lo porta.

6.88. La relación entre colaboradores, visitantes, proveedores de Fruno y guardas de seguridad debe ser estrictamente laboral y bajo un marco de respeto en ambos sentidos. Ante el incumplimiento de este punto en cualquiera de las

partes, Fruno realizará la investigación correspondiente y aplicará las acciones que para el caso sean necesarias.

6.89. La recepción de proveedores o personas de mantenimiento debe ser comunicada por la persona que solicita el servicio, al guarda de seguridad, y podrán ingresar y transitar dentro de las instalaciones de la compañía únicamente si cuenta con el gafete de visitante y que se encuentre en compañía del colaborador responsable del servicio que gestiona el proveedor. Es obligación del guarda de seguridad entregar el gafete de visitante al proveedor siempre y cuando éste presente la identificación de la empresa que brinda el servicio a Fruno y deje su identificación personal en la caseta de seguridad, misma que podrá retirar en el momento que abandone la empresa y entregue en buen estado el gafete que la empresa le ha asignado.

6.90. Las visitas que los colaboradores reciban por motivos laborales deben ser comunicadas al guarda de seguridad (seguridad@fruno.com), en donde se les asignará el gafete de visitante, en el entendido de que durante su permanencia en la compañía deberán estar acompañadas del colaborador responsable de recibir al visitante. Lo anterior debe darse en el lapso que contempla un horario de oficina, es decir de 07:30 am a 05:00 de la tarde de lunes a viernes o bien según sea notificado el horario del departamento en cuestión.

6.91. Solamente será permitida una visita por razones laborales fuera del horario mencionado en el punto anterior cuando sea autorizada por alguna de las gerencias de la compañía, en tanto haya en todo momento una jefatura que se responsabilice del cierre del edificio y la activación de la alarma en caso de que el oficial ya haya terminado su turno, para lo anterior deberán hacer comunicación previa, de al menos 24 horas, formal al departamento de recursos humanos.

6.92. Las visitas de carácter personal no están autorizadas para ningún colaborador excepto con autorización previa de RRHH o la gerencia general, caso en el cual deben someterse al mismo control de visitantes.

6.93. Los visitantes, clientes o proveedores que requieran ingresar a las áreas de: producción, taller, bodegas, ingreso, despacho, logística, en compañía del

colaborador, no podrán ingresar con teléfonos celulares o cámaras fotográficas. En caso de requerir imágenes, deben realizar la solicitud por correo electrónico al contacto de la empresa, quién revisará con gerencia si se autoriza o no. Por lo que queda prohibido la grabación de audio y de video.

6.94. El guarda de seguridad debe notificar al jefe de seguridad cualquier irregularidad presentada por parte de los visitantes o proveedores.

6.95. En el entendido de que, quien brinda el servicio a los clientes es Fruno por medio de sus colaboradores, la entrega de presentes o regalías que los clientes deseen brindar a la compañía, especialmente si se tratare de unidades telefónicas o equipo de esta índole, deberán ser coordinadas con la empresa por medio de Gerencia General o Recursos Humanos. Para más información sobre el punto anterior, por favor ver el procedimiento *FR-PO-RH03 Relación entre Colaboradores y Clientes*.

Colaboradores.

6.96. Respetar y acatar los protocolos definidos por la empresa, según sean notificados por RRHH mediante correo electrónico o bien por sus jefaturas.

6.97. Si cambia de celular (el IMEI), debe asegurarse de reportar el cambio a su jefatura, y de que su jefatura realice la actualización en el sistema de marcas.

6.98. Siga los lineamientos relacionados al código de vestimenta, para más información consulte la política, *FR-PO-RH07 Código de vestimenta*.

6.99. Durante la jornada laboral, se prohíbe ingresar a los baños haciendo uso de la gabacha anti estática o pulseras ESD.

6.100. Se invita a todo el personal a crear y mantener un ambiente de convivencia laboral agradable y de respeto.

6.101. Mantener el orden y aseo de sus puestos de trabajo y áreas comunes.

6.102. Se prohíbe fumar dentro de las instalaciones de la empresa (incluye tiendas y quioscos) y de la zona franca.

6.103. Fruno proporcionará un casillero para los/las colaboradores de los departamentos de: producción, taller, bodegas, ingreso, despacho, logística.

6.104. El ingreso y consumo de alimentos y bebidas en las áreas operativas está prohibido. Para áreas operativas, no se permite el ingreso de recipientes o botellas metálicas, sólo se permite ingresar botella plástica, la cual debe ser transparente.

6.105. El personal de las áreas operativas no podrán ingresar a sus áreas de trabajo con: teléfonos celulares, laptop personal, tablets, tarjetas sim, cámaras fotográficas, dispositivos de almacenamiento (memorias usb, disco duros externos), manos libres. Estos deben ser almacenados en el casillero asignado notificando al guarda de seguridad que porta el artículo con el fin de no ser retenido en la revisión.

6.106. Está prohibido realizar grabaciones de video o tomar fotos dentro de las áreas operativas sin autorización por escrito de la jefatura o la gerencia general.

6.107. En los casos en donde algún colaborador requiera hacer el uso de un celular empresarial para ejecutar funciones laborales, debe ser autorizado por su jefatura directa mediante correo electrónico y debe realizar la solicitud al departamento de bodega por el mismo medio, para que el dispositivo le sea entregado, firmando la boleta correspondiente que quedará en custodia del departamento de seguridad. Sólo se permitirán los casos en donde la jefatura haya autorizado por correo electrónico.

6.108. Para los casos en donde se ha asignado un celular para uso laboral dentro de las áreas operativas, entiéndase para uso en funciones propias del puesto, está prohibido el uso de reproductores de música vía streaming, videos vía streaming, uso de redes sociales, nubes de almacenamiento, aplicaciones de música, correos electrónicos personales o no oficiales, aplicaciones de chat o de pedido de alimentos.

6.109. El uso de celulares está permitido para las áreas administrativas de la empresa, o para aquellos colaboradores que por la naturaleza de su trabajo

requiera el uso del celular. Para ello el jefe inmediato debe registrar los celulares en el sistema de marcas.

6.110. Sobre el uso de reproductores de música, debe ser exclusivamente un reproductor de música, que no funcione como USB o tarjeta de memoria externa y que no tenga cámara. De ser tal y como se indica, podrán ingresarlo y mantenerlo en su puesto de trabajo, pero no sacarlo de la empresa sin previa autorización de recursos humanos. Las personas que ingresen con su reproductor, deben dejarlo adentro de la empresa en el entendido de que la empresa no se hará responsable bajo ninguna circunstancia de daño alguno que pueda sufrir.

6.111. Se usarán audífonos exclusivamente de la empresa, por lo tanto, no es permitido que se saquen audífonos del edificio.

6.112. El personal dispondrá de turnos de receso, los cuales deben seguir con el horario asignado por la jefaturas. Además de realizar las marcas correspondientes en el sistema de marcas.

6.113. No se permite la permanencia del personal, que ya haya salido de sus jornada laboral y que se mantenga de forma ociosa dentro de la empresa.

6.114. La empresa podrá realizar revisiones de conocimiento al personal para asegurar que los procesos se cumplen según las especificaciones o procedimientos indicados de forma interna o pos los clientes de Fruno.

Limpieza de áreas de trabajo.

6.115. Fruno cuenta con personal de limpieza para realizar tal labor en las áreas de trabajo, se solicita al personal colaborar con el aseo.

6.116. Antes de ingresar a Fruno, la persona o personas de limpieza serán revisadas por el guarda de seguridad. Para esto el guarda de seguridad de la empresa utilizará el detector de metales antes del ingreso, asegurándose de que la persona de limpieza no porte algún dispositivo de almacenamiento o similar.

6.117. Mientras la persona de limpieza se encuentra dentro del área segura, el supervisor o la jefatura en turno debe estar en el área segura.

6.118. Cuando la persona de limpieza haya terminado sus labores, debe ser revisada por el guarda de seguridad de Fruno a fin de asegurarse que no porte ningún dispositivo exclusivo del área segura o de otras áreas.

6.119. Los basureros colocados en las zonas seguras, deben utilizar bolsas transparentes. Las bolsas de basura serán auditadas por el guarda de seguridad de Fruno cada vez que la persona de limpieza saque la basura del edificio. La revisión se realizará con el detector de metales, en caso de activarse el detector de metales se debe separar la bolsa para una segunda revisión.

6.120. En esta segunda revisión, el guarda debe colocarse guantes de protección y manipular la basura con extremo cuidado. Esto con el fin de detectar si en la basura se encuentran dispositivos, terminales o herramientas sensibles.

6.121. En el caso de que se detecte alguna irregularidad o se encuentren dispositivos, terminales o herramientas durante el proceso de revisión, el guarda de seguridad deberá informar a recursos humanos y al oficial de seguridad.

Revisiones en seguridad.

6.122. Durante la jornada laboral, todo el personal que sale de Fruno (hacia la soda, a la cocina, o los casilleros, etc) deberá ser revisado siempre por el guarda de seguridad, acatando las indicaciones del guarda de seguridad.

6.123. El proceso de seguridad en cuanto al ingreso y salida de los/las colaboradores que haya sido revisado a la hora de su salida y requiere entrar de nuevo a la compañía ya sea para ir al casillero, servicios sanitarios o cualquier diligencia, deberá de realizar nuevamente el proceso de revisión de seguridad sin excepción alguna, volviendo a realizar la fila correspondiente.

6.124. Los tiempos de revisión del personal dependerá únicamente del personal y de las pertenencia que porte al momento de la salida.

6.125. Para más información ver el procedimiento *FR-PO-SE02. Política de revisión del personal.*

Casos de Emergencia.

- 6.126. En caso de emergencia, en donde se deba realizar la evacuación del edificio, se activará el protocolo de la brigada de emergencia de la empresa.
- 6.127. Para ello se brindará la atención correspondiente por medio de la brigada de emergencias y de la comisión de salud ocupacional.
- 6.128. Para su información, el personal de la brigada de emergencia están identificados con un cordón o lanyard de color rojo en el gafete de la empresa.
- 6.129. En caso de emergencia siga las instrucciones de los brigadistas.

Aclaraciones.

- 6.130. Fruno se reserva el derecho de realizar evaluaciones periódicas al azar, relacionadas la seguridad de la empresa, lo anterior a fin de asegurar el adecuado cumplimiento de las normas de seguridad establecidas, de igual forma podrá modificar las políticas y medidas de seguridad o bien realizar revisiones más exhaustivas como por ejemplo hacer auditoria en los casilleros, cada vez que lo considere necesario y sin previo aviso. Lo anterior se hará siempre en presencia del / de la colaborador, recursos humanos y el guarda de seguridad.
- 6.131. Fruno coordinará auditorias internas de seguridad al menos una vez por año con el fin de asegurar el cumplimiento de los puntos indicados.
- 6.132. En caso de que el personal viole los lineamientos de seguridad del presente documento se verá expuesto a la aplicación de acciones disciplinarias tal y como consta en el código de trabajo de Costa Rica.
- 6.133. El incumplimiento de las obligaciones establecidas en la presente política facultará a Fruno a imponer acciones disciplinarias, de conformidad con la gravedad de la falta y del despido según conste la reiteración de la conducta no deseada.

Control de versiones:

Número	Nombre	Detalle	Fecha
1	Jonathan Espinoza	Rev A. Restructuración del documento y asignación al dept. de seguridad.	23/10/2023
2	Mauren Vega	Rev B. Actualización	04/10/2024
3			
4			
5			
6			
7			
8			
9			
10			