1 Resumen

Securitas tiene como objetivo llevar a cabo siempre sus actividades comerciales de acuerdo con los más altos estándares éticos, *20. El Código de Valores y Ética de Securitas* (el "Código"), así como otras Políticas del Grupo, establecen ciertos valores y principios que Securitas exige a todos sus empleados y socios comerciales que siempre se adhieran en su trabajo para Securitas.

Securitas promueve una cultura corporativa en la que los empleados informan abiertamente a la dirección de los problemas que les preocupan en el lugar de trabajo. Sin embargo, los empleados a veces no quieren denunciar, o se sienten incómodos informando abiertamente, de cuestiones que preocupan a la dirección, por ejemplo, por miedo a las represalias. El conocimiento de las preocupaciones es crucial para garantizar que Securitas pueda resolver los problemas potenciales sin demora.

El objetivo de esta política de denuncia de irregularidades (la "**Política**") y sus instrucciones obligatorias es establecer el marco principal para gestionar los informes o quejas de mala conducta presentados por empleados o terceros contra un empleado, director o funcionario de Securitas sin temor a represalias. La mala conducta puede incluir violaciones de las leyes o regulaciones o el incumplimiento de una política, instrucción o código de ética y valores de Securitas.

Resumen de los principales cambios desde la última revisión:

Sin cambios.

2 Texto principal de la política

Securitas anima a todos los empleados, socios comerciales u otros terceros a denunciar cualquier conducta indebida sospechada o conocida. Las inquietudes deben plantearse de buena fe y pueden informarse de manera confidencial o anónima. Los informes de mala conducta deben describir con el mayor detalle posible el presunto comportamiento poco ético, las personas involucradas y la base y la evidencia de la acusación. Cuando sea posible, se deben proporcionar pruebas documentales de respaldo.

Esta política cubre el planteamiento de preocupaciones relacionadas con incumplimientos del Código de Valores y Ética de Securitas, las políticas corporativas, así como las leyes y reglamentos.

La denuncia de infracciones se puede realizar de muchas maneras, la más común de las cuales es la presentación de informes a un gerente local, un representante de recursos humanos, un oficial de cumplimiento de ética empresarial, un asesor general o un jefe de gerente legal / de riesgos.

Con el fin de facilitar la denuncia en situaciones más delicadas, Securitas también ha establecido la "Línea de Integridad de Securitas" (disponible en securitas.integrityline.com), que es un sistema de gestión de cumplimiento basado en la web que permite **la denuncia anónima,** operado por un proveedor externo. La Línea de Integridad de Securitas es

gestionada por Securitas AB, siguiendo las reglas de esta Política, para garantizar la integridad del sistema y salvaguardar la información reportada.

Debido a la legislación local de protección de datos (entre otras cosas), no todos los asuntos pueden ser reportados a través del tipo de procesamiento de datos que implica la Línea de Integridad de Securitas. Con el fin de salvaguardar el procesamiento de informes que no se pueden gestionar a través de la Línea de Integridad de Securitas, Securitas también opera un sistema en papel para presentar y procesar quejas. Este sistema sigue los mismos principios que la versión electrónica de la Línea de Integridad de Securitas y busca alcanzar el mismo nivel de integridad y responsabilidad.

Un elemento fundamental de esta política es que Securitas no tolera ninguna represalia contra las personas que han informado de sus preocupaciones de buena fe. Este servicio de denuncia de irregularidades es seguro, confidencial, imparcial y está disponible a todas horas; Los denunciantes pueden denunciar de forma anónima, aunque eso puede dificultar la investigación de la inquietud.

Todos los asuntos reportados serán investigados de manera exhaustiva, objetiva y oportuna y de acuerdo con las instrucciones obligatorias relacionadas con esta Política. Los asuntos reportados se manejan sin la influencia de las personas que están o podrían verse afectadas por la queja.

El Consejero Delegado del Grupo emitirá nuevas directivas o procedimientos en relación con la denuncia de irregularidades. Se puede delegar la tarea de emitir instrucciones o procedimientos adicionales.

3 Aplicabilidad

La Política se aplica a todos los empleados y entidades del Grupo Securitas.

La Política está sujeta a la ley aplicable. Cuando los términos de esta Política, en comparación con la ley aplicable, proporcionen salvaguardas, derechos o recursos más fuertes o adicionales para los empleados, prevalecerán los términos de esta Política. Debido a las normas y regulaciones significativamente diferentes sobre el procesamiento de datos y la integridad (así como otras áreas relevantes) en los países de Securitas, las subsidiarias de Securitas pueden adoptar políticas locales complementarias que establezcan las desviaciones necesarias de la Política debido a las regulaciones locales. Dichas políticas deben ser aprobadas por el Director de Cumplimiento de Ética Empresarial.

4 Implementación y responsabilidad

Es responsabilidad de todos los Presidentes de División, del Asesor Jurídico de la División y, a través de ellos, de cada Presidente de País (o equivalente) y del Jefe de Asuntos Jurídicos/Asesor Jurídico local y de la persona responsable de BE, garantizar que esta Política (y la legislación local pertinente) se comprenda e implemente plenamente en sus áreas o países de responsabilidad.

Securitas AB tiene la responsabilidad general del procesamiento de datos dentro de la Línea de Integridad de Securitas, pero la responsabilidad final recae en cada país individual que permite el procesamiento de datos para sus empleados en el sistema. Entre Securitas AB y

las entidades jurídicas locales, así como con el Proveedor Externo (tal y como se define a continuación), se firman Contratos de Tratamiento de Datos que regulan los derechos y obligaciones entre las partes.

5 Capacitación

La formación sobre cómo plantear preocupaciones está incluida en el curso de e-learning de Valores y Ética, que es obligatorio para todos los empleados.

6 Investigaciones y consecuencias del incumplimiento

Securitas anima y espera que todos los empleados y socios comerciales informen de incidentes de incumplimiento relacionados con posibles violaciones de las leyes, reglamentos o políticas de la empresa (incluido el Código) utilizando los canales identificados en esta Política, ya sea que se relacionen con Securitas, sus empleados o sus socios comerciales.

Securitas tiene tolerancia cero con la mala conducta ética, y el personal cuya conducta infrinja los requisitos de la Política puede enfrentarse a medidas legales y disciplinarias, incluida la rescisión del empleo.

7 Revisión y seguimiento

El cumplimiento de esta política por parte de todas las entidades y empleados de Securitas será monitoreado como parte del Programa de Cumplimiento de Ética Empresarial.

8 Referencia a las instrucciones

El CEO ha emitido las siguientes instrucciones relacionadas con los informes de integridad:

- 26.1. Instrucciones a la Política de Denuncia de Irregularidades

26.1 Instrucciones sobre la política de denuncias de irregularidades de Securitas

1 Introducción y objetivo

El propósito de estas instrucciones obligatorias es establecer un proceso estándar sobre cómo se manejarán las denuncias de mala conducta presentadas por empleados o terceros contra un empleado, director o funcionario de Securitas.

Resumen de los principales cambios desde la última revisión:

- Cambios menores en la descripción del proceso de investigación.
- Aclaración de las personas responsables del grupo.
- Se menciona específicamente que los países deben establecer sus propios procesos, de acuerdo con esta instrucción.

2 Cómo denunciar

Los informes o quejas de mala conducta pueden realizarse a través del sistema confidencial de denuncias de Securitas, Integrity Line, a través de los canales de denuncia normales, como Gerente, representante de RRHH, Oficial de Cumplimiento de Ética Empresarial, Asesor General de División o Jefe de Asuntos Legales/Asesor Jurídico, Gerente de Riesgos, o enviando un correo electrónico a integrity@securitas.com.

2.1 Informes dentro de la Línea de Integridad de Securitas

Securitas Integrity Line, es administrada por un proveedor externo (el "**Proveedor Externo**")

Se puede presentar una denuncia sobre mala conducta a la Línea de Integridad de Securitas, ya sea:

(i) A través de Internet en securitas.integrityline.com (fuera de EE. UU., Canadá y México)
(ii) Vía www.securitashotline.com para los EE. UU., www.securitashotline.ca para Canadá y www.lineadealerta.com.mx para México
(iii) Por teléfono a los números detallados en el sitio respectivo (solo para EE. UU., Canadá y México).

Si la persona denunciante indica que desea permanecer en el anonimato, la Línea de Integridad le informará de que la denuncia anónima puede dificultar la realización de una investigación detallada de la denuncia o la presunta infracción. Securitas anima a los denunciantes a proporcionar sus datos de contacto cuando planteen preocupaciones éticas para que sea más fácil obtener información adicional.

Si la persona denunciante insiste en permanecer en el anonimato, y esto no está prohibido por la legislación local, la identidad de la persona denunciante solo será revelada por el Proveedor Externo a Securitas o a un tercero, si:

a) La persona denunciante ha accedido de antemano a revelar su identidad, o
b) Es requerido por la ley o por un interés público importante.

La Línea de Integridad de Securitas proporcionará al denunciante los medios que le permitan verificar el estado de la queja o violación denunciada y dejar información adicional o responder a las preguntas (voluntariamente) planteadas por los investigadores (si corresponde).

Si los informes se reciben por teléfono, el Proveedor Externo redactará un registro y presentará un informe en la Línea de Integridad de Securitas. El informe mencionará la fecha en que el empleado reportó la queja o la supuesta violación del Código.

El denunciante tendrá acceso al informe a través de un código de inicio de sesión mientras el informe permanezca abierto y podrá complementar y solicitar cambios en el informe utilizando este código de inicio de sesión. Si la persona denunciante ha solicitado permanecer en el anonimato, la denuncia no contendrá el nombre de la persona denunciante.

2.2 Informes fuera de la Línea de Integridad de Securitas

Una queja fuera de la Línea de Integridad de Securitas y los canales normales de denuncia puede presentarse abierta o anónimamente a Securitas de la siguiente manera (pero no limitado a):

- Por teléfono, correo electrónico, correo postal o en persona a un gerente local, representante de recursos humanos, oficial de cumplimiento de ética empresarial, asesor general de división o jefe de gerente legal/de riesgos.
- Por teléfono, correo electrónico, correo postal o en persona a un Gerente Divisional o Regional, un representante de Recursos Humanos Divisional, un Oficial de Cumplimiento de Ética Empresarial o un Gerente Legal/de Riesgos Divisional o Regional.
- Por correo electrónico a la siguiente dirección: integrity@securitas.com.
- Por correo ordinario a: Chief Business Ethics Compliance Officer, P.O. Box 12307, S-102 28 Estocolmo, Suecia.

2.2.1 Notificación al grupo

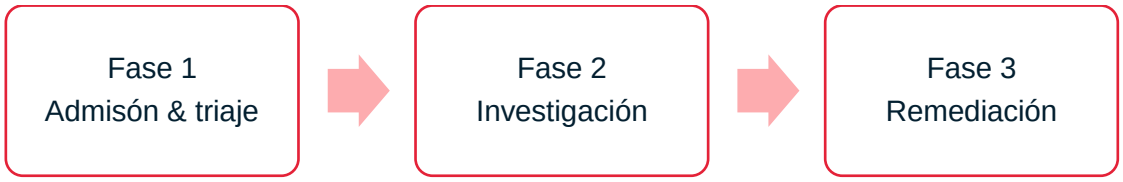
Todos los informes de mala conducta realizados fuera de la Línea de Integridad de Securitas deben notificarse a la función de Ética Empresarial del Grupo y seguir el proceso de investigación estándar que se describe a continuación en la Sección 3. El Equipo de Ética Empresarial del Grupo debe ser notificado de todos los casos de riesgo alto o medio lo antes posible, y el caso debe registrarse en la línea global de Integridad de Securitas. Los casos de bajo riesgo pueden notificarse trimestralmente o según lo solicite el equipo de Ética Empresarial del Grupo.

Un caso puede clasificarse como de riesgo alto o medio si se refiere a una violación de la ley, del Código de Valores y Ética de Securitas o de las políticas corporativas, o si de alguna otra manera se considera un problema grave. Un caso puede clasificarse como de bajo riesgo si, por ejemplo, se refiere principalmente a una queja personal

relacionada con el trabajo. Póngase en contacto con el BECO de la División si tiene dudas sobre cómo categorizar un caso específico.

3 Investigaciones

Todos los informes de mala conducta pasarán por el mismo proceso de tres etapas que se describe a continuación:



3.1 Fase de admisión y triaje

Todos los informes o quejas de mala conducta en la Línea de Integridad de Securitas y enviados a integrity@securitas.com se dirigirán inicialmente al Director de Cumplimiento de Ética Empresarial (CBEO) y a los Oficiales de[1] Cumplimiento de Ética Empresarial de la División (BECO). La CBEO, junto con las BECO, revisará el informe y programará una evaluación de triaje para priorizar las investigaciones de los informes que indiquen riesgos materiales graves. La fase de admisión y triaje seguirá la sección 3.4. Requisitos de tiempo.

Como resultado de la clasificación, se puede incluir a personas independientes relevantes (generalmente el Asesor Jurídico General y/o el Jefe de Recursos Humanos) para confirmar y acordar la evaluación inicial cuando sea necesario.

Si el informe se refiere a personas en la gerencia de la División, el Asesor General del Grupo debe estar involucrado, y la evaluación de triaje puede completarse sin el aporte de la División.

La evaluación de triaje dará lugar a la decisión de:

a. Solicita más información,
b. Investigar el caso, o
c. Desestime el caso

Solicitud de más información: si durante la fase de triaje, el CBEO o los BECO consideran que se requiere más información para decidir cómo proceder, se comunicarán con el informante. El informante tendrá entonces 2 semanas para proporcionar más información.

Investigar el caso : si se toma la decisión de investigar, el informe o la queja se asignará a un administrador de casos. El Administrador de Casos será determinado por la evaluación del nivel de riesgo realizada durante la fase de triaje. Si el caso se considera de alto riesgo, entonces el Administrador del Caso será el CBEO o el BECO Divisional respectivo. Para los casos de riesgo medio, el Administrador de Casos será el Personal

[1] Los protocolos individuales de admisión e investigación pueden ser acordados entre la función de Ética Empresarial y una División y una Unidad de País/Negocio.

de la División, Legal, ICFR o BECO (ver 3.1.1), o el responsable local con supervisión de la División. Finalmente, en general los casos de bajo riesgo serán manejados directamente por Personas locales, Legales o Responsables de BE.

El Gestor de Casos puede ser un empleado interno independiente de Securitas o un investigador externo. La decisión del Grupo de asignar el caso será la autorización del Administrador del Caso para llevar a cabo la investigación.

El Administrador de Casos planificará, llevará a cabo e informará sobre la investigación. El personal de la división respectiva (por ejemplo, Legal, ICFR, HR o BECO) puede ser consultado cuando sea necesario y puede actuar como un segundo par de ojos (principio de los cuatro ojos) y puede brindar asesoramiento sobre el plan de investigación y el informe, verificando el riesgo legal y otras cuestiones.

Desestimar el caso: si el informe no proporciona información suficiente o adecuada, después del período de 2 semanas, el caso será desestimado. Se informará al informante en caso de que desee proporcionar más información en una etapa posterior.

3.1.1 Responsables del grupo

Para los casos de riesgo medio y alto, los respectivos gerentes responsables de la División o del Grupo (ICFR, Personas, Legal) participarán durante la etapa de triaje y mantendrán la supervisión de la investigación para abordar cualquier posible inquietud.

Las respectivas funciones divisionales (por ejemplo, RRHH, BE y Legal) son responsables del análisis y seguimiento de los casos en la Línea de Integridad de Securitas a nivel agregado. El objetivo del seguimiento es garantizar que los casos se gestionen de manera oportuna y adecuada y que se aborden adecuadamente las tendencias. Las funciones de las divisiones también supervisarán y prestarán asistencia a los países en la tramitación de los casos.

Todos los asuntos reportados serán investigados de manera exhaustiva, objetiva y oportuna. Los asuntos reportados se manejan sin la influencia de las personas que están o podrían verse afectadas por la queja.

3.2 Fase de investigación

Una investigación será administrada por el Administrador de Casos, quien seguirá un proceso de investigación estándar con cuatro pasos separados. Los detalles de cada paso se describirán en detalle en un Manual del Administrador de Casos por separado[2]. Los pasos de la investigación se describen aquí y se describen con más detalle a continuación:

[2] Además, se pondrán a disposición plantillas de investigación y documentación.

3.2.1 Paso 1: Evaluar: ¿Merece el asunto una investigación?

Antes de que el administrador de casos comience a planificar la investigación, debe hacer una evaluación inicial sobre las acusaciones en el informe y sobre la asignación del caso.

Antes de continuar con el siguiente paso, el Administrador de Casos debe:

1. Ser claro sobre la presunta mala conducta que se va a investigar y el enfoque de la investigación.
2. Tener suficientes detalles en la acusación para tener una línea inicial de investigación.
3. Haber realizado una verificación preliminar de algunos elementos.
4. Haber regresado con el reportero para obtener más información, si es necesario.
5. No tener intereses personales que puedan interferir con su objetividad en el caso.

En el caso de que se trate de un reporte clasificado como de bajo riesgo y el Administrador de Casos no considere que el asunto amerita una investigación, debe consultar con la respectiva Función Divisional y documentar adecuadamente el razonamiento detrás de la decisión en el sistema de la Línea de Integridad de Securitas. En caso de que el informe se califique como de riesgo alto o medio, el administrador del caso debe obtener la aprobación del BECO Divisional antes de cerrar el caso.

Cuando el administrador de casos haya confirmado lo anterior 1-5 y haya evaluado que se requiere una investigación, puede continuar con el siguiente paso.

3.2.2 Paso 2 Planifique qué, quién, cuándo, dónde y cómo

Una investigación es un proceso de responder a la siguiente pregunta: ***"¿los hechos respaldan una acusación o no?"*** El enfoque de una investigación está en los hechos, no en opiniones, hipótesis o rumores.

Cada investigación depende de los hechos únicos relacionados con las acusaciones, pero como regla general, los investigadores deben mantener una mente abierta, ser minuciosos, desafiar a los testigos sobre los hechos, buscar los detalles, entrevistar a todos los testigos relevantes, revisar todos los documentos relevantes y no aceptar declaraciones sin verificación.

En este paso, el Administrador de Casos debe establecer un plan de investigación para identificar los hechos que son relevantes para la presunta mala conducta. El plan comienza con un análisis de quién hizo qué, cómo, cuándo y dónde, y debe documentarse en la Línea de Integridad de Securitas para casos de riesgo alto y

medio. El plan de investigación para los casos de bajo riesgo puede documentarse localmente en el país.

Si se considera necesario realizar una búsqueda en la cuenta de correo electrónico de un empleado actual o anterior o revisar otros archivos, por ejemplo, registros financieros o estados de cuenta de tarjetas de crédito, es posible que esto deba aprobarse por separado.

El Administrador de Casos documentará el plan en la Línea de Integridad de Securitas para casos de riesgo alto o medio. Si existen riesgos o requisitos legales específicos que puedan aplicarse en la jurisdicción, el administrador de casos debe consultar con la función divisional respectiva para asegurarse de que el plan sea adecuado para su propósito. En el caso de informes clasificados como de bajo riesgo, el plan de investigación puede documentarse fuera de la Línea de Integridad de Securitas, sin embargo, se alienta al Administrador de Casos a buscar asesoramiento de las Funciones Divisionales si es necesario.

3.2.3 Paso 3: Conducta: recopile los hechos siguiendo el plan

En este paso, el Administrador de Casos ejecuta las acciones identificadas en el plan. La clave para implementar un plan exitoso es desglosar cada una de las acciones en una actividad, generalmente encontrando información en documentos o correos electrónicos o a través de entrevistas a personas.

Las actividades llevadas a cabo en la investigación deben proporcionar respuestas a las preguntas planteadas en el plan, es decir, quién hizo qué, cómo, cuándo y dónde.

Al realizar una investigación es importante que el conocimiento del caso se limite a la menor cantidad de personas posible. Esto es importante por tres razones; La presunta mala conducta aún no está justificada y, por lo tanto, debemos respetar la dignidad y la reputación de la persona que ha sido acusada de mala conducta. En segundo lugar, queremos proteger al denunciante de posibles represalias. Por último, si ha habido mala conducta, es posible que la persona en cuestión tome medidas para eliminar pruebas o alterar la investigación de otro modo.

3.2.4 Paso 4: Informe - Informe de los hechos en relación con la acusación

El propósito de la investigación es conocer los hechos y sacar conclusiones sobre si una acusación de mala conducta está fundamentada o no, y cuando esté fundamentada, tomar medidas para corregir el comportamiento y/o sus consecuencias.

Una vez finalizada la investigación, es necesario reunir los hechos en un informe escrito. El informe debe incluir registros de entrevistas y evidencia de búsquedas de documentos u otros registros. El informe también debe proponer una conclusión sobre si el caso está fundamentado o no y propuestas de reparación. El informe constituirá la base para la posterior discusión y decisión de la gerencia con respecto a las consecuencias que puedan resultar del caso.

En todos los casos recibidos a través de la Línea de Integridad de Securitas, el informe debe documentarse en el sistema de la Línea de Integridad de Securitas. El informe final, en el caso de los casos de riesgo alto o medio, siempre debe ser examinado por las funciones pertinentes de la División antes de que concluya la fase de investigación y se inicie la siguiente fase de reparación.

Si la conclusión es que el caso no está fundamentado, el administrador del caso debe informar al reportero que el caso ha sido investigado, pero que no pudimos encontrar hechos que corroboren las acusaciones, y el caso puede cerrarse.

3.3 Fase de remediación

La reparación es la acción tomada para remediar las causas y consecuencias de una mala conducta comprobada y es el objetivo principal del proceso de investigación.

La fase de remediación comienza con la difusión del informe de investigación a los líderes empresariales correspondientes sobre una base estricta y confidencial de necesidad de conocimiento, y a las respectivas personas responsables del Grupo. Los líderes empresariales correspondientes pueden solicitar la participación de otro personal funcional, como el Jefe de Finanzas, el Asesor General/Jefe de Asuntos Legales o el Jefe de Recursos Humanos.

Para revisar el informe, el administrador de casos designado convoca a una reunión de remediación con la participación de los líderes empresariales correspondientes, según lo definido en la descripción del proceso local. La Función Divisional responsable podrá ser invitada y deberá participar en caso de casos de alto o mediano riesgo.

En la reunión se presenta el informe y los participantes evalúan el hallazgo y las propuestas de remediación. La discusión sobre la corrección comienza con los hallazgos y las propuestas de reparación identificados en el informe de investigación, pero la reunión también debe realizar un análisis de la causa raíz para comprender las fallas que causaron que se presentara el informe o la queja con el propósito de evitar que vuelva a suceder.

El resultado de la reunión de remediación debe ser acordar un plan de remediación que debe contener detalles sobre:

- Las acciones correctivas acordadas,
- El/los gerente/s responsable(s) de la implementación de las acciones,
- Plazos para la implementación de las acciones, y
- Seguimiento posterior, por ejemplo, después de 6 meses para continuar con el cumplimiento

Las medidas correctivas internas pueden incluir, por ejemplo, medidas disciplinarias, reasignación de personal, recapacitación del personal, revisión de los documentos de dirección pertinentes, mejoras en los controles y procesos internos. Además, puede haber acciones externas como acciones legales contra terceros y la posibilidad de notificación a las autoridades aplicables (por ejemplo, la policía).

En todos los casos recibidos a través de la línea Securitas Integrity, el plan de remediación debe estar documentado en el sistema de la línea Securitas Integrity.

3.3.1 Cerrar el caso

Si la conclusión es que el caso no tiene fundamento, el administrador del caso debe informar al informante que el caso ha sido investigado, pero que no pudimos encontrar hechos que corroboren las acusaciones, y el caso puede cerrarse.

Del mismo modo, cuando se ha acordado el plan de remediación, el Administrador de Casos debe informar al denunciante que el caso ha sido investigado y que la gerencia está tomando las medidas adecuadas.

El Administrador de Casos también puede notificar a los testigos que el caso se está cerrando y recordarles a los testigos el deber de confidencialidad. Los registros de la investigación se mantendrán en el sistema de denuncias, Integrity Line, en caso de que la denuncia original llegara a través de este canal. Los informes de bajo riesgo recibidos a través de otros canales pueden almacenarse localmente según se defina en un proceso local.

3.4 Cronometraje

Las investigaciones deben realizarse de manera oportuna. Los siguientes plazos se aplican a todas las investigaciones:

- *El acuse de recibo de la denuncia debe* enviarse a la persona denunciante lo antes posible y, a más tardar, siete (7) días después de recibir la denuncia. El Equipo de Ética Empresarial es responsable de gestionar este proceso para los informes recibidos a través de la Línea de Integridad de Securitas.
- *La finalización de la investigación y la retroalimentación al denunciante* deben realizarse dentro de los tres (3) meses posteriores a la recepción del informe del denunciante por parte del administrador del caso. (como excepción, las investigaciones altamente complejas pueden extenderse más allá de este período, pero deben ser monitoreadas de cerca por el Grupo o la persona responsable de la división).

4 Protección de datos personales

La información sobre la protección y el tratamiento de datos personales se puede encontrar en el *Anexo 1*.

5 Aplicabilidad

Estas instrucciones son obligatorias y se aplican a todas las empresas, empleados, directores y directivos de las empresas del Grupo Securitas, es decir, empresas en las que Securitas AB (publ), directa o indirectamente, posee o tiene una participación mayoritaria.

6 Implementación y responsabilidad

El Grupo será responsable de gestionar la Línea de Integridad de Securitas y de proporcionar el material de formación y las plantillas necesarias para que los Gestores de Casos lleven a cabo investigaciones. El Grupo también desarrollará material de información estándar para la Línea de Integridad de Securitas y para el proceso de investigación descrito en esta instrucción.

Es responsabilidad de todos los Presidentes de Divisiones y, a través de ellos, de cada Presidente de País, asegurar que esta Política sea plenamente comprendida e implementada en sus áreas o países de responsabilidad.

Cada país debe tener una descripción del proceso, de acuerdo con esta Instrucción, que describa cómo se clasifican, investigan y remedian los casos gestionados localmente. Esta descripción debe incluir tanto la gestión de los casos que llegan a través de la Línea de Integridad de Securitas, como los presentados fuera de la línea de Integridad de Securitas.

El objetivo del proceso es garantizar una investigación independiente y una solución justa y equilibrada para todos los casos gestionados localmente, en función de la legislación local aplicable.

7 Consecuencias del incumplimiento

Las violaciones de estas instrucciones pueden resultar en una acción disciplinaria apropiada para la violación, que incluye, entre otros, la terminación del empleo. También puede dar lugar a multas o sanciones de las que el individuo puede ser considerado responsable.

8 Revisión y seguimiento

El cumplimiento de estas instrucciones por parte de todas las entidades y empleados de Securitas será monitoreado a través de auditorías internas y externas, y seguimientos rutinarios de todos los asuntos reportados.

_____

Anexo 1

Protección de datos personales

Para obtener información sobre qué empresa de Securitas está procesando su información y cómo ponerse en contacto con nosotros, consulte el documento Controladores de datos personales, que puede encontrar al final de este documento en el apéndice.

El documento de Controladores de Datos Personales también cubre cualquier enmienda o modificación a este Aviso de Privacidad que se aplique a un país específico, los llamados Términos Únicos de País. Si una parte del Aviso de Privacidad se modifica mediante Términos Únicos de País específicos, el resto del Aviso de Privacidad permanece sin cambios. Los cambios relevantes se enumeran debajo de cada país, si no se enumera nada, no hay variaciones locales.

En Securitas ("**Securitas**", "**nosotros**" o "**nos**") respetamos su integridad. Este Aviso de Privacidad para la Línea de Integridad de Securitas describe cómo recopilamos y procesamos datos personales en relación con nuestra plataforma de informes confidencial y segura, que se puede utilizar para informar incidentes y plantear preocupaciones sobre mala conducta, irregularidades, violación de leyes, regulaciones o incumplimiento de las políticas aplicables de Securitas. Para leer más sobre nuestro Código de Valores y Ética, visite el mosaico del código de Valores y Ética.

Es importante para nosotros que lea y comprenda este Aviso de Privacidad antes de utilizar la Línea de Integridad de Securitas. Le invitamos a ponerse en contacto con nosotros si tiene alguna pregunta.

Responsabilidad del tratamiento de los datos personales

La entidad local pertinente de Securitas que ha recibido el informe del incidente junto con Securitas AB son corresponsables (corresponsables del tratamiento) del tratamiento de datos personales en la Securitas Integrity Line. Para garantizar la protección de sus datos personales, hemos celebrado un acuerdo conjunto con respecto al uso y la protección de sus datos personales. Este Aviso de Privacidad refleja la esencia de nuestro acuerdo conjunto. Si desea más información sobre el acuerdo, puede ponerse en contacto con nosotros.

Categorías de datos personales

La información que se describe a continuación se procesará en relación con el uso de Securitas Integrity Line y cualquier investigación de un informe de incidente presentado. Las categorías de datos personales que se tratarán en el caso concreto

dependen del contenido del informe del incidente, de la información proporcionada por el denunciante y de la información que se considere pertinente para la investigación.

Además, el sistema de denuncia permite a un denunciante presentar denuncias y comunicarse de forma anónima a través de una conexión cifrada, en cuyo caso no se recogerá ningún dato personal, como punto de partida, del denunciante, a menos que el denunciante proporcione voluntariamente datos personales en la notificación del incidente como tal o en una comunicación posterior.

Características Personales e Identificadores: Nombre y apellidos.

Información del directorio personal: dirección de correo electrónico, número de teléfono, secuencias de video, imágenes o grabaciones de voz

Información de contacto de la empresa: Su función, título, la empresa para la que trabaja.

Información de incidentes y casos: Detalles sobre el incidente reportado, el ID de caso designado.

Comunicación: Contenido de correos electrónicos, mensajes u otras comunicaciones.

Datos del Audit Trail (Información técnica): dirección IP, versión del sistema operativo y navegador.

La finalidad y la base jurídica del tratamiento

Securitas está procesando los datos personales que usted, como *denunciante*, nos proporciona cuando utiliza la Línea de Integridad de Securitas, se comunica con los administradores de casos o que recopilamos de otras fuentes en relación con una investigación de un incidente.

Las fuentes de las que recopilamos datos personales en relación con un informe de incidente y una investigación de un incidente incluyen, además de la persona denunciante, la(s) persona(s) denunciada(s), otras personas (que pueden ser empleados u otro personal comprometido o personas externas) involucradas en una investigación, asesores legales, autoridades públicas y fuentes de información disponibles públicamente, por ejemplo, información disponible en Internet o registros públicos.

Finalidad del tratamiento	**Base legal para el procesamiento**	**Periodo de conservación**
Procesamos los datos personales descritos	*La empresa Securitas responsable de*	Los datos personales

anteriormente para recopilar, gestionar e investigar los informes de incidentes presentados a través de la Línea de Integridad de Securitas, lo que incluye revisar y evaluar el informe, comunicarnos con el denunciante y otras personas relevantes para la investigación del informe del incidente y documentar las medidas adoptadas para investigar el incidente denunciado.	*investigar la denuncia:* En la medida en que la empresa Securitas esté legalmente obligada a recopilar y gestionar informes de incidentes, el tratamiento es necesario para cumplir con una obligación legal. Cuando no exista una obligación legal para la empresa Securitas de recopilar y gestionar incidentes, la empresa Securitas se basa en su interés legítimo para gestionar los informes de incidentes e investigar presuntas conductas indebidas, irregularidades, violaciones de leyes, reglamentos o incumplimiento de las políticas aplicables de Securitas. *Securitas AB y otras empresas relevantes de Securitas:* El tratamiento es necesario para satisfacer el interés legítimo de Securitas AB y de la empresa Securitas correspondiente de gestionar los	recopilados en relación con un informe de incidente se almacenarán para este propósito durante la investigación de un incidente y durante un período de dos (2) años a partir de la fecha en que se cerró el caso.

	informes de incidentes e investigar presuntas conductas indebidas, irregularidades, violaciones de leyes, reglamentos o incumplimiento de las políticas aplicables de Securitas.	
Procesamos la información de incidentes y casos recopilada a través de la Línea de Integridad de Securitas para analizar los informes de incidentes a nivel agregado y producir estadísticas.	El tratamiento es necesario para satisfacer el interés legítimo de Securitas AB y de la empresa Securitas correspondiente de analizar los informes de incidentes a nivel agregado y producir estadísticas. Esto nos ayuda a comprender mejor, por ejemplo, cuántos informes de incidentes se envían a través de la plataforma de informes y qué tipos de incidentes se notifican.	Para este fin, los datos personales se almacenan durante el mismo período que se almacenan los informes de incidentes en la plataforma de informes, lo que significa que los datos personales se almacenarán durante un período de dos (2) años a partir de la fecha en que se cerró el caso. La información a nivel agregado y las estadísticas que no incluyen ningún dato personal pueden almacenarse hasta nuevo aviso o hasta que se eliminen.
Tratamos y compartimos los datos personales pertinentes con las autoridades públicas, las empresas del grupo Securitas, los asesores jurídicos, los sindicatos y los comités de empresa	El tratamiento es necesario para satisfacer el interés legítimo de Securitas AB y de la empresa Securitas correspondiente en la gestión y defensa de	Para ello, los datos personales se conservan durante el período necesario para que podamos gestionar y defender la

cuando sea necesario para gestionar y defender las reclamaciones legales derivadas de la notificación de un incidente. Esto incluye informar del incidente a las fuerzas del orden cuando corresponda.	reclamaciones legales.	reclamación legal en el caso concreto.
Procesamos los datos personales almacenados en la Línea de Integridad de Securitas para garantizar la funcionalidad técnica y la seguridad del sistema de informes, lo que incluye garantizar que solo los administradores de casos autorizados accedan a los datos personales de la Línea de Integridad de Securitas, en relación con el registro para la resolución de problemas y la gestión de incidentes y para mantener copias de seguridad de los datos personales para garantizar la disponibilidad de los datos personales procesados en caso de un problema técnico o físico.	El tratamiento es necesario para satisfacer el interés legítimo de Securitas AB y de la empresa Securitas correspondiente de garantizar la funcionalidad técnica y la seguridad del sistema de informes.	Los datos personales se almacenan para este fin durante los mismos períodos descritos anteriormente.

¿Con quién compartimos sus datos personales?

EQS Group: Sus datos personales serán procesados por nuestro proveedor de servicios EQS Group AG ("**EQS Group**"), que proporciona la plataforma de informes utilizada para la Securitas Integrity Line y sus subprocesadores (que proporcionan, por ejemplo, servicios de alojamiento y traducción) siguiendo las instrucciones de Securitas. EQS Group AG actúa como procesador de datos personales de Securitas y, en virtud de acuerdos contractuales, solo está autorizado a procesar datos para los fines establecidos anteriormente. EQS Group no tiene acceso a los informes de incidentes en la plataforma de informes, a menos que Securitas lo autorice específicamente.

Otros proveedores de servicios: Además, en relación con la investigación de un informe de incidentes, sus datos personales serán procesados por otros proveedores de servicios o subcontratistas que hayamos contratado, incluidos los proveedores de servicios de almacenamiento de datos y los proveedores de herramientas de productividad y comunicación, cuando el administrador de casos utilice herramientas proporcionadas por dichos proveedores de servicios para llevar a cabo la investigación. Todos los proveedores de servicios y subcontratistas actúan como procesadores de datos personales de Securitas y, en virtud de acuerdos contractuales, solo se les permite procesar datos para los fines autorizados por Securitas. Además, el encargado del tratamiento de datos personales (proveedor de servicios o subcontratista) y aquellos que actúen siguiendo las instrucciones del encargado del tratamiento no accederán a más datos personales de los necesarios para la prestación del servicio objeto del acuerdo con Securitas.

Grupo Securitas: Cuando un informe de incidente se refiera a otra empresa del Grupo Securitas, los datos personales recopilados en relación con un informe de incidente podrán compartirse con la empresa Securitas si es necesario para investigar el incidente y, cuando sea necesario, para gestionar y defender reclamaciones legales como resultado de un informe de incidente.

Autoridades públicas: Securitas comparte sus datos personales con las autoridades públicas (como la policía, la autoridad fiscal u otras autoridades) cuando sea necesario para gestionar y defender reclamaciones legales. Las autoridades públicas que reciban sus datos personales serán las responsables de dicho tratamiento, lo que significa que no es Securitas quien rige cómo se procesan sus datos personales si se comparten con una autoridad. Por lo tanto, si sus datos personales se comparten con las autoridades, este Aviso de Privacidad no cubrirá ese procesamiento posterior.

Asesores legales: Cuando sea necesario para gestionar y defender reclamaciones legales como resultado de un informe de incidentes, compartimos datos personales con asesores legales que hemos contratado. Normalmente, el asesor jurídico es responsable (responsable del tratamiento) de su propio tratamiento de datos personales cuando presta asesoramiento y servicios jurídicos.

Compañías de seguros: Cuando sea necesario para gestionar y defender reclamaciones legales como resultado de una notificación de incidentes, compartimos datos personales con compañías de seguros, por ejemplo, para presentar una reclamación de seguro como resultado de un incidente (según corresponda). La compañía de seguros es responsable (controlador) de su propio procesamiento de datos personales cuando se gestiona un reclamo o asunto de seguro.

Sindicatos y comités de empresa: Securitas comparte datos personales, cuando sea necesario, con sindicatos y comités de empresa para gestionar y defender reclamaciones legales como resultado de una denuncia de incidentes, incluida la adopción de medidas de derecho laboral (advertencias y terminación de empleo con o sin aviso), en su caso, contra la persona denunciada. Los sindicatos y los comités de

empresa son responsables (controladores) de su propio tratamiento de datos personales.

Dónde procesamos sus datos personales

Para proporcionarle la Línea de Integridad de Securitas, nosotros y EQS Group, que procesa datos personales en nuestro nombre, procesamos su información principalmente dentro de la UE/EEE. Hemos firmado términos de confidencialidad y procesamiento de datos con EQS Group para garantizar que cumplan con los altos niveles de confidencialidad, las leyes de protección de datos y las mejores prácticas en estándares de privacidad y seguridad.

Sin embargo, si utiliza Securitas Integrity Line desde un país fuera de la UE/EEE (un tercer país), sus datos personales se transferirán al país desde el que acceda a Securitas Integrity Line.

Además, determinados servicios relacionados con la plataforma de presentación de informes, por ejemplo, los servicios de traducción, son prestados por subcontratistas del Grupo EQS en terceros países. Para garantizar que sus datos estén suficientemente protegidos fuera de la UE, nos hemos asegurado de que existan las salvaguardias adecuadas, incluidas las Cláusulas Contractuales Tipo (CCT) de la UE, para garantizar un nivel de protección esencialmente equivalente para sus datos personales.

Cómo protegemos sus datos

Securitas y EQS Group toman las medidas técnicas y organizativas adecuadas para proteger sus datos personales en la plataforma de informes y garantizar que sus datos personales estén seguros en la plataforma. Los datos personales procesados en la plataforma de informes se almacenan encriptados en una base de datos segura. Además, la comunicación entre su navegador web y la plataforma de informes está encriptada para garantizar que sus datos personales estén protegidos contra la divulgación o el acceso no autorizados. Solo los administradores de casos autorizados tendrán acceso a los informes de incidentes en la plataforma de informes.

Sus derechos

Respetamos su integridad y sus derechos en virtud de la legislación relacionada con el tratamiento de datos personales. Los derechos que tiene significan que puede solicitar una copia de los datos personales que procesamos sobre usted, solicitar que se corrija la información incorrecta sobre usted e incluso bajo ciertas condiciones, solicitar la eliminación de la información.

En ciertas jurisdicciones, sus derechos pueden estar restringidos, por ejemplo, el derecho a una copia de sus datos personales, dado que un informe de incidente y las investigaciones como resultado de un informe de incidente presentado están sujetos

a confidencialidad según la ley. Esto con el fin de proteger a la persona denunciante y a otras personas involucradas en una investigación de un informe de incidente.

Además, no se aplica el derecho a la portabilidad de los datos, ya que el tratamiento de los datos personales no se basa en un acuerdo con usted ni en su consentimiento, como se muestra en la tabla anterior. Por último, Securitas considera que, normalmente, no se puede oponerse con éxito al tratamiento de datos personales en la plataforma de denuncias, dada la naturaleza y la finalidad del tratamiento.

Para ejercer sus derechos, no dude en ponerse en contacto con su entidad local de Securitas a través de los datos de contacto proporcionados en el documento de Controladores de Datos Personales, que puede encontrar al final de este documento en el apéndice.

También tiene siempre derecho a presentar reclamaciones ante la Autoridad Sueca para la Protección de la Privacidad (o su equivalente nacional) si tiene objeciones a nuestro tratamiento de sus datos personales.