



**STEEL SEGURIDAD PRIVADA LTDA.**

**SU SEGURIDAD ES NUESTRO COMPROMISO**

NIT. 830.106.318-4



**Versión: 01**

**MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y  
RECUPERACIÓN DE LOS DATOS.**

**MA-GQ-01**




**MANUAL DE SEGURIDAD INFORMÁTICA,  
PROTECCIÓN Y RECUPERACIÓN DE LOS  
DATOS.**

**ESTAMOS CONTRIBUYENDO CON LA CONSERVACION DEL MEDIO AMBIENTE**

Fecha de Edición o Actualización Dic.- 2016

Proceso: Sistemas de Gestión Integrado

	<p><b>STEEL SEGURIDAD PRIVADA LTDA.</b>  <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b>  NIT. 830.106.318-4</p> 	<p><b>Versión: 01</b></p>
<p><b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y  RECUPERACIÓN DE LOS DATOS.</b></p>		<p><b>MA-GQ-01</b></p>

## 1.1 PRESENTACIÓN DE LA ORGANIZACIÓN

## 1.2 RESEÑA HISTORICA



STEEL SEGURIDAD PRIVADA LTDA, con NIT 830106318-4 es una empresa que presta servicios de vigilancia y seguridad privada en las modalidades de vigilancia fija, móvil, escoltas y medios tecnológicos, creada por escritura pública No 1261 del 27 de junio de 2002 en la notaria cincuenta y cinco de Bogotá y su domicilio principal se encuentra en la ciudad de Santiago de Cali; registrada en la Cámara de Comercio de esta ciudad el 24 de septiembre de 2009 bajo el No. 11064 del libro IX, con matrícula mercantil No 775176-3 de fecha 28 de septiembre de 2009, Resolución N° 20131200053657 del 29 de agosto 2013.

## 1.3 UBICACIÓN GEOGRÁFICA

La sede principal de la empresa STEEL SEGURIDAD PRIVADA LTDA, está ubicada en la ciudad de Cali, en la dirección: Calle 3 No. 61ª - 08 Barrio Pampalinda. Además, contamos con sedes en la ciudad de Pasto, Armenia y Buenaventura. Teléfonos 397-57-56 385-37-76 correo steelseguridad@gmail.com. www.steelseguridad.co

## 1.4 SERVICIOS QUE SE PRESTAN

- ✓ Vigilancia y seguridad privada con armas (modalidad fija o móvil)
- ✓ Servicio de vigilancia privada sin armas (modalidad fija o móvil)
- ✓ Servicio de escolta a personas, vehículos y mercancías
- ✓ Estudios de seguridad.
- ✓ Medios tecnológicos.

 <b>STEEL SEGURIDAD PRIVADA LTDA.</b> <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b> NIT. 830.106.318-4 	<b>Versión: 01</b>
<b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b>	<b>MA-GQ-01</b>

## **2 PLANIFICACIÓN ESTRATÉGICA**

### **2.1 MISIÓN:**

Brindar soluciones en seguridad privada, con personal competente en el que los valores humanos sean la base fundamental de la excelencia en el servicio.

### **2.2 VISIÓN:**

Para el 2020 posicionarnos como una empresa reconocida por los sectores productivos en seguridad integral en el mercado nacional.



### **2.3 VALORES CORPORATIVOS**

Son lineamientos que rigen a STEEL SEGURIDAD PRIVADA LTDA en el desempeño de las actividades y en la identidad de su cultura organizacional.

**HONESTIDAD:** Honradez en el proceder frente a todas las actividades del entorno empresarial.

**RESPONSABILIDAD:** Puntual cumplimiento a los compromisos adquiridos, realizando de manera correcta las actividades encomendadas.

**EFFECTIVIDAD:** Búsqueda permanente de la excelencia en la realización de las actividades empresariales para cumplir con los objetivos organizacionales.

 <b>STEEL SEGURIDAD PRIVADA LTDA.</b> <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b> NIT. 830.106.318-4 	<b>Versión: 01</b>
<b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b>	<b>MA-GQ-01</b>



### 3 INTRODUCCIÓN.

La seguridad informática o seguridad de tecnologías de la información es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore (activo) y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último solo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

 <b>STEEL SEGURIDAD PRIVADA LTDA.</b> SU SEGURIDAD ES NUESTRO COMPROMISO NIT. 830.106.318-4 	<b>Versión: 01</b>
<b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b>	<b>MA-GQ-01</b>

## 4 OBJETIVO

Indicar a los empleados de la organización el procedimiento a seguir en el manejo y uso de todos los elementos relacionados con equipos de informática y correo electrónico, para el desarrollo de actividades o cargos asignados y de sus funciones a realizar dentro de STEEL Seguridad Privada Ltda

## 5 ALCANCE


Se aplica para todo el personal de la organización que utilice los equipos de informática y correo electrónico

## 6 REFERENCIA

NTC – ISO 27000

## 7 DEFINICIONES

- **ARCHIVO ADJUNTO:** Es un archivo que se transmite junto a un mensaje de correo electrónico.
- **BUZÓN DE CORREO:** Área para almacenar los mensajes de correo electrónico provenientes de un servidor.
- **CORREO ELECTRÓNICO:** Es un servicio de red que permite a usuarios enviar y recibir mensajes mediante sistemas de comunicación electrónica.
- **DOMINIO:** Es un nombre base que agrupa a un conjunto de equipos o dispositivos, que permite proporcionar nombres de equipo más fácil de recordar que una dirección numérica de Internet.
- **FREEWARE:** Tipo de software de computadora que se distribuye sin coste y por tiempo ilimitado, siendo una variante gratuita del shareware, en el que la meta es lograr que un usuario pague, usualmente después de un tiempo de prueba ("trial") limitado y con la finalidad de habilitar toda la funcionalidad. A veces se incluye el código fuente, pero no es lo usual.

 <b>STEEL SEGURIDAD PRIVADA LTDA.</b> <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b> NIT. 830.106.318-4 	<b>Versión: 01</b>
<b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b>	<b>MA-GQ-01</b>



- **HARDWARE:** Cualquier componente físico tecnológico, que trabaja o interactúa de algún modo con la computadora. No sólo incluye elementos internos como el disco duro, CD-ROM, disquetera, sino que también hace referencia al cableado, circuitos, gabinete, etc. E incluso hace referencia a elementos externos como la impresora, el mouse, el teclado, el monitor y demás periféricos.
- **INTERNET:** Es una red mundial con millones de servidores conectados. Estos pueden intercambiar información y establecer distintos servicios tales como visitar páginas de portales, correo electrónico, charlar por medio del teclado en los salones creados para este servicio, entre otros.
- **INTRANET:** Red propia de una organización, diseñada y desarrollada siguiendo los protocolos propios de Internet, en particular el protocolo TCP/IP. Puede tratarse de una red aislada, es decir no contactada a Internet.
- **SHAREWARE:** Modalidad de distribución de software, tanto como juegos como programas utilitarios, para que el usuario pueda evaluar de forma gratuita el producto, por un tiempo especificado, aunque también las limitaciones pueden estar en algunas de las formas de uso o las capacidades finales.
- **SOFTWARE:** Conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en una computadora.
- **USUARIO:** Persona, oficina, organización o grupo de personas a quien la organización asigna una cuenta de trabajo en el domino.

## 8 ACTIVIDADES.

A continuación se plantean una serie de recomendaciones que pretende garantizar su correcta utilización, disponibilidad y nivel de servicio de los recursos informáticos de STEEL Seguridad Privada Ltda


### 8.1 Equipos Informáticos.

- El equipo solo puede ser usado para fines de la organización y para apoyo de las actividades del trabajo del usuario.

	<p><b>STEEL SEGURIDAD PRIVADA LTDA.</b>  <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b>  NIT. 830.106.318-4</p> 	<p><b>Versión: 01</b></p>
<p><b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b></p>		<p><b>MA-GQ-01</b></p>

- El computador debe tener los programas con su licencia de funcionamiento y los iconos o accesos directos solo de los programas que sean necesarios para el cumplimiento de las funciones al cargo asignado.
- La instalación de software, freeware, shareware como Yahoo! Messenger, MSM, etc., el usuario debe solicitar la autorización del personal calificado para hacerlo y que esto será solamente utilizado en beneficio de la actividad organizacional.
- No es permitido la instalación software o programas que provengan del exterior Internet o medios físicos como disquete, USB o CD-ROM.
- Todo tipo de archivos, programas, freeware, shareware, sin su respectiva autorización de su uso, serán eliminados de su PC o equipo de Informática.
- La revisión de los equipos PC o de informática, se hará en forma periódica, para verificar su buen funcionamiento y que los programas instalados sean los que solo la Organización necesita para realizar las funciones asignadas, (como mínimo cada seis meses).
- La configuración, revisión de cualquier componente de hardware o software del PC o equipo de informática, labores de mantenimiento preventivo, etc. sólo puede ser realizada por el proveedor autorizado por la Gerencia General o Coordinación Administrativa.
- Todo equipo debe tener la protección en la parte eléctrica con un estabilizador, regulador, o UPS. Sin esto no podrá hacer la utilización del PC o equipo de Informática.
- La instalación o descarga de archivos de música en cualquier tipo de formato está prohibida; estos, así como aquellos archivos que no tengan relación alguna con el trabajo que realiza en la Organización, si estos no están autorizados, serán eliminados PC o equipo de Informática.
- Se prohíbe a los empleados de la organización, el ingreso y salida de información por medio de disquetes, unidad de U.S.B. y/o CD-ROM.



	<p><b>STEEL SEGURIDAD PRIVADA LTDA.</b>  <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b>  NIT. 830.106.318-4</p> 	<p><b>Versión: 01</b></p>
<p><b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y  RECUPERACIÓN DE LOS DATOS.</b></p>		<p><b>MA-GQ-01</b></p>

- El sitio de trabajo de su PC o equipo de Informática debe tener los estándares de soporte, comodidad tanto para el PC o equipo de Informática, como para el usuario, así como su aseo general del sitio o ubicación del mismo.
- El tomar líquidos, comer cualquier tipo de alimentos en el puesto de trabajo del PC o equipo de Informática está totalmente prohibido.

## **8.2 Correo Electrónico.**

### **8.2.1 Normas por parte de los usuarios.**


#### **8.2.1.1 Volumen**

Cada empleado que use el servicio de correo electrónico incide directamente en el rendimiento de la red de datos de la Organización, la cual tiene una capacidad limitada y la carga excesiva sobre esta red puede causar interrupciones y demoras en la transmisión de datos críticos y prioritarios para el negocio.

Algunas recomendaciones sobre la forma de reducir el volumen del correo generado, son las siguientes:

- Los mensajes deberían enviarse únicamente a esas personas que realmente necesiten recibir la información.
- Evite reenviar mensajes que contienen cadenas, avisos de un nuevo y peligroso virus, desacreditar marcas y productos, ya que ellos sólo buscan alimentar las listas de correo del sitio que los originan y en algunos casos simplemente, congestionar el tráfico en algunos tramos de la red.
- Evite el envío de material pornográfico y pida a sus contactos que se abstengan de enviárselo.
- En los últimos años, la infraestructura de mensajería electrónica se ha beneficiado de mejoras en cuanto al rendimiento y confiabilidad. Sin embargo, la demanda en el uso del correo también se ha incrementado. Se requiere que los usuarios aseguren que el volumen del correo electrónico no exceda la capacidad de nuestro sistema.



	<p><b>STEEL SEGURIDAD PRIVADA LTDA.</b>  <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b>  NIT. 830.106.318-4</p> 	<p><b>Versión: 01</b></p>
<p><b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b></p>		<p><b>MA-GQ-01</b></p>

- Hay varias cosas que se esperan de nuestros usuarios. Ante todo, esperamos la buena administración de los buzones de correo.
- Desarrolle el hábito de borrar los mensajes viejos e innecesarios periódicamente.
- Configure su programa de correo para que elimine los mensajes definitivamente cada vez que decida salir del programa. Recuerde que los mensajes que se borran van a residir a la carpeta de “mensajes eliminados”.
- Minimice el hábito de adjuntar archivos a los mensajes que podrían ser enviados usando texto plano dentro del cuerpo del mensaje.


#### 8.2.1.2 Abuso

La mensajería electrónica, es suministrada únicamente para propósitos de negocio. La Organización reconoce que algún correo personal será inevitable, sin embargo, tal correspondencia debería permanecer la menor cantidad de tiempo almacenada y su envío y recepción también deberían ser mínimos. La solicitud y/o distribución de material que no esté relacionado con el negocio, particularmente aquel del que se obtiene un beneficio personal, está estrictamente prohibido.

El abuso del correo electrónico es un problema serio y es considerado de la misma forma que el abuso de equipos e información de propiedad de STEEL Seguridad Privada Ltda El correo electrónico no está exento de las consideraciones sociales, éticas y legales que nos convierten en ciudadanos responsables.

Los empleados de STEEL Seguridad Privada Ltda, deben asegurarse de no usar el correo electrónico para:

- Representarse ellos mismos como otras personas.
- Transmitir o almacenar material que podría ser considerado inapropiado, ofensivo o irrespetuoso a los demás.
- Transmitir o almacenar videos, imágenes y/o texto considerado pornográfico.

	<p><b>STEEL SEGURIDAD PRIVADA LTDA.</b>  <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b>  NIT. 830.106.318-4</p> 	<p><b>Versión: 01</b></p>
<p><b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b></p>		<p><b>MA-GQ-01</b></p>

- Transmitir o almacenar mensajes obscenos o amenazantes.
- Originar o retransmitir las cartas conocidas como “cadenas”.
- Acosar, hostigar o asediar a otros empleados.
- Proveer información acerca de lista de los empleados de la Organización a terceros.
- Participar en actividades que interfieren con su trabajo o el trabajo de otros empleados.
- Interferir con la operación del sistema de mensajería de STEEL Seguridad Privada Ltda
- Violar cualquier ley o derechos de cualquier persona.
- Instar, apoyar o promover la afiliación con un partido político o persona.
- Generar mensajes para beneficio personal.

Los empleados no deberían presentar puntos de vista o ideas como representantes de la organización, a menos que lo estén haciendo como parte de la función que desempeñan dentro de STEEL Seguridad Privada Ltda Los usuarios necesitan recordar que ellos son siempre identificables cuando expresen puntos de vista personales deberán siempre hacer claridad de cuando se están representando a ellos mismos o lo hacen en nombre de STEEL Seguridad Privada Ltda

Los empleados no deben nunca deliberadamente generar mensajes que dañen, inhabiliten o interrumpan parcial o totalmente el servicio de mensajería electrónica de STEEL Seguridad Privada Ltda

#### 8.2.1.3 Seguridad.

STEEL Seguridad Privada Ltda ha delegado en sus empleados la libertad para generar y recibir mensajes sin excesiva vigilancia por tal razón es conveniente tener en cuenta las siguientes consideraciones:

**ESTAMOS CONTRIBUYENDO CON LA CONSERVACION DEL MEDIO AMBIENTE**



	<p><b>STEEL SEGURIDAD PRIVADA LTDA.</b>  <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b>  NIT. 830.106.318-4</p> 	<p><b>Versión: 01</b></p>
<p><b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b></p>		<p><b>MA-GQ-01</b></p>

- La organización depende de sus colaboradores para el tratamiento adecuado de información o asuntos delicados y el impacto que pudiera generar su distribución. Los mensajes que contiene en ese tipo de información recibida por socios de negocios, competidores, y/o el público en general, pueden causar daños serios a la organización. La discreción debe ser usada cuando se establezcan comunicaciones con empleados que no pertenecen a la Organización.
- En particular, la información “privada” y “confidencial” nunca debe ser transmitida fuera de la organización pues de ninguna manera garantiza la privacidad de la mensajería electrónica.
- El siguiente extracto resume la política de la organización respecto a la privacidad de los mensajes electrónicos. “Todo correo electrónico, conferencia de datos, y correo de voz almacenado sobre un equipo de la organización es considerado de propiedad de STEEL Seguridad Privada Ltda Por lo tanto, los funcionarios asignados para tal fin, pueden periódicamente chequear el contenido de los mensajes almacenados en tales equipos ya sea porque se requiere corregir problemas de la red o simplemente para establecer el uso apropiado de los mensajes recibidos o generados. Usted no puede esperar privacidad personal de los mensajes enviados, recibidos o almacenados en esos equipos”.
- Las cuentas de mensajería electrónica están normalmente protegidas por una contraseña, la cual reduce el riesgo de acceso por parte de los intrusos. Esta protección, sin embargo, no confiere ninguna característica especial a los mensajes almacenados en equipos de propiedad de la Organización y por tanto serán susceptibles de ser controlados por la organización.

Para este control de seguridad EL Representante ante la Gerencia del Sistema de Gestión en Control y Seguridad, tendrá en sobre cerrado las claves de cada uno de los equipos que la organización tiene.

### **8.2.2 Normas por parte de STEEL Seguridad Privada Ltda**

Se asignará una cuenta por usuario.

 <b>STEEL SEGURIDAD PRIVADA LTDA.</b> <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b> NIT. 830.106.318-4 	<b>Versión: 01</b>
<b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b>	<b>MA-GQ-01</b>

- La cuenta se dará de baja en el momento que el personal deje de pertenecer a la organización.
- La organización se reserva el derecho de enviar al usuario la información que considere necesaria por el correo electrónico, como un medio de comunicación organizacional.
- La vigencia y espacio de las cuentas será definido por la Gerencia General y/o la Coordinación Administrativa de acuerdo a los recursos disponibles, con base en las necesidades del usuario.

### **8.3 Internet e Intranet**



#### **8.3.1 Internet.**

Desde el equipo asignado a cada usuario será posible hacer uso de la red de Internet, únicamente para fines de interés laboral y no personal.

#### **8.3.2 Intranet**

La utilización de freeware, shareware como Yahoo! Messenger, MSM, etc está autorizada por la organización para servicio de intranet o herramienta de comunicación en beneficio de la actividad organización, manejado dentro del horario laboral en las instalaciones de STEEL Seguridad Privada Ltda

El cambio de red o suspensión de esta será autorizado por la Gerencia General. La política adoptada sobre el uso de correo electrónico será de igual aplicación para otros recursos de la intranet y el Internet.

 <b>STEEL SEGURIDAD PRIVADA LTDA.</b> <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b> NIT. 830.106.318-4 	<b>Versión: 01</b>
<b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b>	<b>MA-GQ-01</b>

### 8.3.3 Copias de Seguridad – Backup.

El objetivo del Backup es proteger los datos y aplicaciones de software contra todo tipo de fallas que puedan ocurrir y posibilitar la recuperación de fallas en el menor tiempo posible y sin la pérdida de datos.

Entre los archivos que deben tener copias de respaldo se destacan:

- Backup de los documentos y correos de cada equipo en el dominio
- Backup del Sistema de Contabilidad
- Backup del Sistema de Gestión en Control y Seguridad
- Backup de los sistemas operativos

La copia de seguridad se realiza diariamente en forma magnética y la copia se almacena fuera de STEEL Seguridad Privada Ltda. Adicionalmente algunos archivos, especialmente de carácter operativo y Sistemas de Gestión, cuenta, con protección de almacenamiento virtual para ser consultados en cualquier momento.


### 8.3.4 Claves

Los equipos de cómputo tienen una clave para su ingreso. Su cambio se realizará cada tres (3) meses y está a cargo del Asistente Administrativo en Buenaventura, Auxiliar Administrativo en Cali y Coordinador de Servicios en Pereira, estas claves de acceso al equipo son conocidas por el administrador para un control sobre los equipos, el administrador es el único que puede cambiar las claves.

## 8.4 Responsabilidades

Los usuarios son responsables de cumplir los puntos señalados en este documento para el mejor manejo de los recursos informáticos.

La Coordinación Administrativa con el apoyo del Asistente Administrativo es responsable de la correcta utilización de los equipos de cómputo, del servidor de correo, de la cuenta de correo, del Internet y del software con los que cuenta la organización.

 <b>STEEL SEGURIDAD PRIVADA LTDA.</b> <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b> NIT. 830.106.318-4 	<b>Versión: 01</b>
<b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b>	<b>MA-GQ-01</b>

## 8.5 Privacidad y confidencialidad de la información.

La organización no realizará monitoreo o inspecciones de un buzón de correo electrónico sin el consentimiento del usuario, salvo en los casos detallados a continuación:

- Algún requerimiento legal.
- Sospecha de violación de la política interna de la organización o de leyes locales, nacionales e internacionales.
- Circunstancias de emergencia, donde no actuar pudiera repercutir gravemente en el servicio general a los clientes y proveedores de STEEL Seguridad Privada Ltda


## 8.6 Acciones Disciplinarias.

Cuando se determine que hubo una violación a lo establecido en este procedimiento, se aplicaran las medidas correctivas y disciplinarias necesarias de acuerdo con la gravedad de la infracción, tomando como base el reglamento interno de STEEL Seguridad Privada Ltda

En caso que el usuario no sea empleado regular de la organización, el Gerente o la persona que éste designe recibirán el asesoramiento pertinente para determinar la acción a seguir.

## 9 SEGURIDAD EN LA RED: PROTECCIÓN DE LA INFORMACIÓN Y DATOS PERSONALES.

La Ley 1273 de 2009 creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.

 <b>STEEL SEGURIDAD PRIVADA LTDA.</b> <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b> NIT. 830.106.318-4 	<b>Versión: 01</b>
<b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b>	<b>MA-GQ-01</b>

El 5 de enero de 2009, el Congreso de la República de Colombia promulgó la Ley 1273 “Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado “De la Protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.

Dicha ley tipificó como delitos una serie de conductas relacionadas con el manejo de datos personales, por lo que es de gran importancia que las empresas se blinden jurídicamente para evitar incurrir en alguno de estos tipos penales.



No hay que olvidar que los avances tecnológicos y el empleo de los mismos para apropiarse ilícitamente del patrimonio de terceros a través de clonación de tarjetas bancarias, vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas cada vez más usuales en todas partes del mundo. Según la Revista Cara y Sello, durante el 2007 en Colombia las empresas perdieron más de 6.6 billones de pesos a raíz de delitos informáticos.

De ahí la importancia de esta ley, que adiciona al Código Penal colombiano el Título VII BIS denominado "De la Protección de la información y de los datos" que divide en dos capítulos, a saber: “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y “De los atentados informáticos y otras infracciones”.

El capítulo primero adiciona el siguiente articulado (subrayado fuera del texto):

Artículo 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.



 <b>STEEL SEGURIDAD PRIVADA LTDA.</b> <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b> NIT. 830.106.318-4 	<b>Versión: 01</b>
<b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b>	<b>MA-GQ-01</b>



Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: DAÑO INFORMÁTICO. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269E: USO DE SOFTWARE MALICIOSO. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269F: VIOLACIÓN DE DATOS PERSONALES. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

 <b>STEEL SEGURIDAD PRIVADA LTDA.</b> <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b> NIT. 830.106.318-4 	<b>Versión: 01</b>
<b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b>	<b>MA-GQ-01</b>

Al respecto es importante aclarar que la Ley 1266 de 2008 definió el término dato personal como “cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica”. Dicho artículo obliga a las empresas un especial cuidado en el manejo de los datos personales de sus empleados, toda vez que la ley obliga a quien “sustraiga” e “intercepte” dichos datos a pedir autorización al titular de los mismos.

Artículo 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Es primordial mencionar que este artículo tipifica lo que comúnmente se denomina “phishing”, modalidad de estafa que usualmente utiliza como medio el correo electrónico pero que cada vez con más frecuencia utilizan otros medios de propagación como por ejemplo la mensajería instantánea o las redes sociales. Según la Unidad de Delitos Informáticos de la Policía Judicial (Dijín) con esta modalidad se robaron más de 3.500 millones de pesos de usuarios del sistema financiero en el 2006[2].

Un punto importante a considerar es que el artículo 269H agrega como circunstancias de agravación punitiva de los tipos penales descritos anteriormente el aumento de la pena de la mitad a las tres cuartas partes si la conducta se cometiere:

- Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
- Por servidor público en ejercicio de sus funciones
- Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.



# STEEL SEGURIDAD PRIVADA LTDA.

SU SEGURIDAD ES NUESTRO COMPROMISO

NIT. 830.106.318-4



Versión: 01

## MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.

MA-GQ-01

- Revelando o dando a conocer el contenido de la información en perjuicio de otro.
- Obteniendo provecho para sí o para un tercero.
- Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
- Utilizando como instrumento a un tercero de buena fe.
- Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.


Es de anotar que estos tipos penales obligan tanto a empresas como a personas naturales a prestar especial atención al tratamiento de equipos informáticos así como al tratamiento de los datos personales más teniendo en cuenta la circunstancia de agravación del inciso 3 del artículo 269H que señala “por quien tuviere un vínculo contractual con el poseedor de la información”.

Por lo tanto, se hace necesario tener unas condiciones de contratación, tanto con empleados como con contratistas, claras y precisas para evitar incurrir en la tipificación penal.

Por su parte, el capítulo segundo establece:

Artículo 269I: HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239[3] manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 del Código Penal [4], es decir, penas de prisión de tres (3) a ocho (8) años.

Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.

 <b>STEEL SEGURIDAD PRIVADA LTDA.</b> <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b> NIT. 830.106.318-4 	<b>Versión: 01</b>
<b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b>	<b>MA-GQ-01</b>

La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

Así mismo, la Ley 1273 agrega como circunstancia de mayor punibilidad en el artículo 58 del Código Penal el hecho de realizar las conductas punibles utilizando medios informáticos, electrónicos o telemáticos.

Como se puede apreciar, la Ley 1273 es un paso importante en la lucha contra los delitos informáticos en Colombia, por lo que es necesario que se esté preparado legalmente para enfrentar los retos que plantea.



En este sentido y desde un punto de vista empresarial, la nueva ley pone de presente la necesidad para los empleadores de crear mecanismos idóneos para la protección de uno de sus activos más valiosos como lo es la información.

Las empresas deben aprovechar la expedición de esta ley para adecuar sus contratos de trabajo, establecer deberes y sanciones a los trabajadores en los reglamentos internos de trabajo, celebrar acuerdos de confidencialidad con los mismos y crear puestos de trabajo encargados de velar por la seguridad de la información.

Por otra parte, es necesario regular aspectos de las nuevas modalidades laborales tales como el teletrabajo o los trabajos desde la residencia de los trabajadores los cuales exigen un nivel más alto de supervisión al manejo de la información.

Así mismo, resulta conveniente dictar charlas y seminarios al interior de las organizaciones con el fin de que los trabajadores sean conscientes del nuevo rol que les corresponde en el nuevo mundo de la informática.

Lo anterior, teniendo en cuenta los perjuicios patrimoniales a los que se pueden enfrentar los empleadores debido al uso inadecuado de la información por parte de sus trabajadores y demás contratistas.

	<b>STEEL SEGURIDAD PRIVADA LTDA.</b> <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b> NIT. 830.106.318-4	 <b>Versión: 01</b>
<b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b>		<b>MA-GQ-01</b>

Pero más allá de ese importante factor, con la promulgación de esta ley se obtiene una herramienta importante para denunciar los hechos delictivos a los que se pueda ver afectado, un cambio importante si se tiene en cuenta que anteriormente las empresas no denunciaban dichos hechos no sólo para evitar daños en su reputación sino por no tener herramientas especiales.

## 10 ACCIONES PREVENTIVAS, DE CONTROL FRENTE A RIESGOS o AMENAZAS DE LA SEGURIDAD INFORMATICA, LA PROTECCIÓN DE LA INFORMACIÓN Y DATOS PERSONALES.

### 10.1 Recomendaciones contra la Acción de Virus.

Es necesario estandarizar el software de antivirus en todas las estaciones de trabajo y servidores. Es aconsejable tener un proveedor de software antivirus para las estaciones y otro diferente para el servidor, para reducir la probabilidad de que un virus que no esté en la lista de actualización, se filtre en toda la red.


Se sugiere que en las estaciones de trabajo se siga con la línea de Karspesky y en el servidor central instalar McAfee.

Por qué tener 2 antivirus diferentes, uno para el servidor y otro para las estaciones de trabajo es porque estos tienen variaciones en sus tablas de definiciones de virus, es más difícil que un virus se propague por la red debido a la diversificación de productos que puedan detectarlos.

Es necesario implementar un procedimiento para las actualizaciones automáticas de las definiciones de virus, tanto para Karspesky como para Macfee. Esta labor la debe realizar el administrador del sistema, cuidando que se ejecute en horas en que no se degrade el performance del tráfico de red.

### 10.2 Recomendaciones Contra Accesos No Autorizados.

Frente a este riesgo potencial, es necesario implementar lo siguiente:

	<p><b>STEEL SEGURIDAD PRIVADA LTDA.</b>  <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b>  NIT. 830.106.318-4</p> 	<p><b>Versión: 01</b></p>
<p><b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b></p>		<p><b>MA-GQ-01</b></p>


### **10.2.1 Recomendaciones a nivel físico.**

- El servidor de archivos no debe ser accesible físicamente a cualquier persona.
- Es conveniente que exista un espacio físico donde se ubique el servidor, con acceso restringido al personal autorizado, y que cumpla con los requisitos adecuados para su funcionamiento, como temperatura ambiental adecuada, aislado del polvo y plagas dañinas.
- En este espacio, además de ubicar el servidor, se pueden ubicar los elementos más sensibles de la red corporativa como el HUB/Switch y el servidor proxy.

### **10.2.2 Recomendaciones a Nivel Lógico.**

- Habilitar un firewall que evite ingresos desde redes externas hacia la red corporativa.
- Instalar un sistema de detección de intrusos para monitorear los accesos o tentativas de accesos a la red corporativa.
- Deshabilitar los servicios que no sean necesarios y luego de esto verificar los posibles puertos que se encuentren abiertos innecesariamente para proceder a cerrarlos.
- Concienciar a los usuarios de la red, se deberá concienciar a los usuarios de la red, acerca de una política mínima de seguridad, por ejemplo, evitar las claves fácilmente descifrables.
- Solo está permitido instalar en las computadoras el software requerido para el desarrollo de las actividades de la empresa.
- Teniendo presente que la mayoría de los ataques informáticos no vienen de fuera, sino de dentro, según lo indican las estadísticas de penetración a las redes corporativas expuestas en el anexo D, un usuario interno podría capturar contraseñas con una herramienta sniffer.



	<p><b>STEEL SEGURIDAD PRIVADA LTDA.</b>  <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b>  NIT. 830.106.318-4</p> 	<p><b>Versión: 01</b></p>
<p><b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y  RECUPERACIÓN DE LOS DATOS.</b></p>		<p><b>MA-GQ-01</b></p>

Para evitarlo, es conveniente que la red, en lugar de estar basada en un HUB, esté basada en conmutador (SWITCH). Eso evitará que todos los paquetes de información lleguen a todas las tarjetas de red. Usando una red conmutada puede evitar muchos intentos de espionaje de la información que circula por la red.

- Es recomendable agregar contraseña del BIOS a todos los equipos de la red, para evitar vulnerabilidades de acceso dependientes de los Sistemas Operativos Instalados.

### **10.2.3 Recomendaciones Para Prevenir Fallas En Los Equipos.**


- La primera opción será designar a uno o más empleados a que dediquen un tiempo para el aprendizaje y formación, mediante la toma de un curso, para que ellos sean los encargados en brindar mantenimiento preventivo y correctivo a los equipos que posee la empresa o contar con una persona con ese perfil.

Como otra opción es importante contar con los servicios de una empresa o un profesional que de forma periódica realice mantenimiento preventivo a los equipos y correctivo si lo amerita la situación.

Sea la decisión que aplique se sugiere que como mínimo se realice por lo menos una vez al año y llevar un control, de la vida útil de los diferentes dispositivos.

- Para evitar el caos que provocaría una avería en el servidor de archivos, o en uno de sus discos duros, plantéese la utilización de un clúster.
- Un sistema de alimentación sin interrupciones (UPS) es hoy en día imprescindible, al menos para el servidor de archivos, el servidor proxy y el HUB/Switch.



	<p><b>STEEL SEGURIDAD PRIVADA LTDA.</b>  <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b>  NIT. 830.106.318-4</p> 	<p><b>Versión: 01</b></p>
<p><b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b></p>		<p><b>MA-GQ-01</b></p>

#### **10.2.4 Recomendaciones Contra El Robo De Datos Y Fraude.**


##### **10.2.4.1 Medidas preventivas contra el robo de datos.**

El conocimiento de las señales y los métodos de robo ayudarán a los jefes de área a estar más conscientes de posibles problemas. Aunque las estadísticas de robo de empleados son alarmantes, este riesgo puede reducirse implementando medidas preventivas como:

- Publicar la Política de Seguridad de la empresa.
- Promover el concepto de responsabilidad del empleado.
- Capacitar a los empleados para estar en alerta ante ladrones (y que vean la importancia del robo a la empresa).
- Estricto proceso de selección del personal. (Exigir certificado de antecedentes, Revisar bien sus referencias.)
- Capacitar bien a los empleados nuevos en los procedimientos.
- Dar énfasis a las políticas de seguridad de la empresa.
- Mantener un ambiente de trabajo limpio y ordenado.
- Desarrollar buenos canales de comunicación con los empleados para resolver quejas.
- Capacitar a los empleados para que tengan una carrera profesional dentro de la empresa.

##### **10.2.4.2 Como prevenir ataques de ingeniería social.**

Para comprobar si se están realizando ataques de este tipo se recogerán estadísticas de incumplimiento de procedimientos. Por ejemplo, analizar el número de personas que han llamado a la empresa y que no se les ha entregado la información porque no proporcionaban todos los datos de identificación solicitados. Poder reconocer ciertas señas típicas de una acción de esta naturaleza, como son rehusarse a entregar información de contacto, tener mucho apuro, referenciar a una persona importante, intimidación o requerimiento de información olvidada, por enumerar las más comunes, es claramente otra manera de estar alertas. De cualquier forma, en la actualidad, es vital educar, capacitar, sensibilizar sobre las políticas y procedimientos definidos y que son relativos a este tema.

 <b>STEEL SEGURIDAD PRIVADA LTDA.</b> <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b> NIT. 830.106.318-4 	<b>Versión: 01</b>
<b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b>	<b>MA-GQ-01</b>

Una forma de defensa contra estos ataques es conocer los conceptos básicos que pueden ser utilizados contra una persona o la compañía a la que pertenece y que abren brechas para conseguir datos. Con este conocimiento se debe adoptar una actitud proactiva que alerte y concienciar a los empleados que avisen de cualquier pregunta o actitud sospechosa. Eso sí, las políticas de seguridad deben ser realistas con reglas concisas y concretas que se puedan cumplir.

#### 10.2.4.3 Protección para correos corporativos.

Se recomienda el uso de una herramienta que permita implementar infraestructura de clave pública para proteger la comunicación por correo electrónico que implique el envío de información confidencial.

#### 10.2.4.4 Recomendaciones sobre cómo realizar las actualizaciones de parches de seguridad.

Como complemento a las sugerencias anteriores, es recomendable estar al día con la instalación de los diferentes parches de seguridad para el software de la empresa.

Debido a que la mayoría de equipos funcionan bajo ambiente Microsoft, es conveniente instalar un servidor, que realice las funciones de actualización de los parches de seguridad de los sistemas operativos Windows instalados en la red. Para esto se configuraría el servidor central para que descargue las actualizaciones y las almacene en disco duro, luego los clientes (estaciones de la red) automáticamente realizarían la actualización conectándose a este servidor. Este proceso se debería ejecutar en horarios que no afecten el desempeño de la red.

También se deben descargar los parches de seguridad para las demás aplicaciones que se utilizan en la empresa, como los productos Oracle, de manera que se esté al día con las correcciones de las vulnerabilidades existentes.

Las recomendaciones de lo que debe realizarse en el caso de presentarse una contingencia como fuego, terremoto o un robo físico, se las podrá encontrar a continuación en el plan de contingencias.

 <b>STEEL SEGURIDAD PRIVADA LTDA.</b> <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b> NIT. 830.106.318-4 	<b>Versión: 01</b>
<b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b>	<b>MA-GQ-01</b>

## 11 PLAN CONTINGENCIA.

El Plan de Contingencias o Emergencias, constituye el instrumento principal para dar una respuesta oportuna, adecuada y coordinada a una situación de emergencia causada por fenómenos destructivos de origen natural o humano.

Sin embargo, es fundamental contar con la suma de esfuerzos, de todos, cuya composición permita fortalecer y cumplir en tiempo las acciones tendientes a prevenir y mitigar desastres en modo y tiempo las circunstancias señaladas y dar respuesta oportuna a las contingencias que se presenten.

Es por ello que se presenta en el siguiente plan, las actividades a tomar en cuenta por cada uno de los funcionarios de STEEL SEGURIDAD PRIVADA LTDA, tanto antes, durante y después de la contingencia.

### 11.1 Actividades Previas Al Desastre, Siniestro O Riesgo.



Son todas las actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de la información, las cuales nos asegurarán un proceso de Recuperación para STEEL SEGURIDAD PRIVADA LTDA con el menor costo posible. A continuación detallaremos las siguientes a realizar:

#### 11.1.1 Establecimiento de plan de acción.

En esta fase de planeamiento se debe de establecer los procedimientos y normas a seguir relativos a:

##### a) Instalaciones físicas de la empresa.

En caso de que se pueda suscitar un robo, sismo o incendio se deberían tomar las siguientes medidas preventivas:



 <b>STEEL SEGURIDAD PRIVADA LTDA.</b> <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b> NIT. 830.106.318-4 	<b>Versión: 01</b>
<b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b>	<b>MA-GQ-01</b>

✓ **Robos:**

- Al entrar y salir de las instalaciones se deberá observar previamente de que no exista ningún individuo sospechoso.
- Queda prohibido dar información personal de los empleados o información confidencial de la organización.
- Contar con personal para resguardo de las instalaciones de la empresa.
- Instalación de alarma.
- Contratar con pólizas de seguros.

✓ **Sismos:**

- Ubicar y revisar periódicamente, que se encuentren en buen estado las instalaciones de AGUA, y SISTEMA ELECTRICO.
- Fijar a la pared repisas, cuadros armarios, estantes, espejos y libreros. Evitar colocar objetos pesados en la parte superior de éstos, además asegurar al techo las lámparas.
- Debe de existir y ubicarse en un lugar de fácil acceso y visible los números telefónicos de emergencia y un botiquín, de ser posible un radio portátil y una linterna con pilas.
- Todo el personal debería portar siempre una identificación.
- Realizar simulacros de manera periódica.


	<p><b>STEEL SEGURIDAD PRIVADA LTDA.</b>  <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b>  NIT. 830.106.318-4</p> 	<p><b>Versión: 01</b></p>
<p><b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b></p>		<p><b>MA-GQ-01</b></p>

✓ **Incendios:**

- Estar siempre alerta. La mejor manera de evitar los incendios, es la prevención.
- Procurar no almacenar productos inflamables.
- Cuidar que los cables de los aparatos eléctricos se encuentren en perfectas condiciones.
- No se deben realizar demasiadas conexiones en contactos múltiples, para evitar la sobre carga de los circuitos eléctricos.
- Por ningún motivo mojar las instalaciones eléctricas. Recuerde que el agua es un buen conductor de la electricidad.
- Todo contacto o interruptor debe tener siempre su tapa debidamente aislada.
- Antes de salir de STEEL SEGURIDAD PRIVADA LTDA la última persona en hacerlo, deberá revisar que los aparatos eléctricos estén apagados o perfectamente desconectados.
- Que prohibido fumar en las instalaciones de STEEL SEGURIDAD PRIVADA LTDA debido a que este habito contaminante, no deja una buena impresión en los clientes y puede causar desagrado ante los no fumadores o puede causar un incendio.
- Bajo ningún motivo se debe sustituir los fusibles por alambre o monedas, ni usar cordones eléctricos dañados o parchados.
- Contar con una alarma de incendios.
- Tener en un lugar visible y accesible un extintor contra incendios.
- Realizar simulacros de manera periódica.
- Debe de existir y ubicarse en un lugar de fácil acceso y visible los números telefónicos de emergencia y un botiquín.


✓ **Equipos de cómputo**

- Inventario actualizado de los equipos de manejo de información (computadoras, impresoras, etc.), especificando su contenido (software que usa) y su ubicación.

 <b>STEEL SEGURIDAD PRIVADA LTDA.</b> <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b> NIT. 830.106.318-4 	<b>Versión: 01</b>
<b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b>	<b>MA-GQ-01</b>

- STEEL SEGURIDAD PRIVADA LTDA podría optar por la toma de una Póliza de Seguros Comerciales, como parte de la protección de los Activos Institucionales, pero haciendo la salvedad en el contrato, que en casos de siniestros, la restitución del Computador siniestrado se podrá hacer por otro de mayor potencia (por actualización tecnológica), siempre y cuando esté dentro de los montos asegurados.
  - Se deberá realizar una señalización o etiquetado de los Computadores de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación. Por ejemplo etiquetar (colocar un stickers) de color rojo al Servidor, color amarillo a las computadoras con Información importante o estratégica y color verde a las computadoras de contenidos normales.
- ✓ **Obtención y almacenamiento de los respaldos de información (BACKUPS o Copias de Seguridad).**
- Se obtendrán copias de Seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los Sistemas o aplicativos de la Institución. Para lo cual se debe contar con:
    - Backups del Sistema Operativo.
    - Backups del Software Base - Paquetes y/o Lenguajes de Programación.
    - Backups de Productos Desarrollados (Considerando tanto los programas fuentes, como los programas objetos correspondientes).
    - Backups de los Datos (Bases de Datos, Índices, y todo archivo necesario para la correcta ejecución de los Productos Desarrollados).
    - Backups del Hardware, mediante convenio con otra Institución que tenga equipos similares o mayores y que brinden la seguridad de poder continuar con las actividades para ser puestos a nuestra disposición, al ocurrir una contingencia y mientras se busca una solución definitiva al siniestro producido. Este tipo de convenios debe tener tanto las consideraciones de equipamiento como ambiente y facilidades de trabajo.





 <b>STEEL SEGURIDAD PRIVADA LTDA.</b> <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b> NIT. 830.106.318-4 	<b>Versión: 01</b>
<b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b>	<b>MA-GQ-01</b>

- Para realizar los respaldos se tendrá en consideración el uso de las herramientas de encriptación que vienen incluidas en el sistema operativo para que la información pueda ser recuperada sola y exclusivamente por quién la generó. También se recomienda tener duplicidad en los respaldos, esto es, mantener un respaldo “in situ” para mayor facilidad de recuperación, y otro respaldo fuera de las instalaciones de la empresa.



✓ **Políticas (normas y procedimientos de Backups).**

- El valor que tiene la información y los datos es casi absoluto, si falla el disco duro, el daño puede ser irreversible, puede significar la pérdida total de nuestra información, por esta razón debemos respaldar la información importante. La pérdida de información provoca daño de fondo como los mencionados a continuación:
  - Pérdida de oportunidades de negocio
  - Clientes decepcionados
  - Reputación perdida
- Las interrupciones se presentan de formas muy variadas: virus informáticos, fallos de electricidad, errores de hardware y software, caídas de red, hackers, errores humanos, incendios, inundaciones. Y aunque no se pueda prevenir cada una de estas interrupciones, STEEL SEGURIDAD PRIVADA LTDA sí puede prepararse para evitar las consecuencias que éstas puedan tener ya que del tiempo que tarde en reaccionar STEEL SEGURIDAD PRIVADA LTDA dependerá la gravedad de sus consecuencias. En parte para reducir el tiempo de recuperación del desastre se tendrán ciertas normas y procedimientos. Seguiremos las siguientes medidas técnicas para la realización de las copias de seguridad, condicionadas de acuerdo a los siguientes puntos:
  - **Volumen de información a copiar :**
  - Sugerimos las siguientes estrategias con respecto a la forma de respaldar la información que puede ser:





 <b>STEEL SEGURIDAD PRIVADA LTDA.</b> <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b> NIT. 830.106.318-4 	<b>Versión: 01</b>
<b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b>	<b>MA-GQ-01</b>

- Copiar sólo los datos: poco recomendable, ya que en caso de incidencia, será preciso recuperar el entorno que proporcionan los programas para acceder a los mismos, influye negativamente en el plazo de recuperación del sistema.
- Copia completa: recomendable, si el soporte, tiempo de copia y frecuencia lo permiten, incluye una copia de datos y programas, restaurando el sistema al momento anterior a la copia.
- Copia incremental: solamente se almacenan las modificaciones realizadas desde la última copia de seguridad, con lo que es necesario mantener la copia original sobre la que restaurar el resto de copias. Utilizan un mínimo espacio de almacenamiento y minimizan el tipo de desarrollo, a costa de una recuperación más complicada.
- Copia diferencial: como la incremental, pero en vez de solamente modificaciones, se almacenan los ficheros completos que han sido modificados. También necesita la copia original.
- **Tiempo disponible para efectuar la copia**
  - El tiempo disponible para efectuar la copia de seguridad es importante, ya que el soporte utilizado, unidad de grabación y volumen de datos a almacenar, puede hacer que el proceso de grabación de los datos dure horas, y teniendo en cuenta que mientras se efectúa el proceso es conveniente no realizar accesos o modificaciones sobre los datos objeto de la copia, por esta razón los respaldos se los deberá realizar fuera del horario laboral.
- **Soporte utilizado**
  - Esta decisión estará condicionada por un conjunto de variables, tales como la frecuencia de realización, el volumen de datos a copiar, la disponibilidad de la copia, el tiempo de recuperación del sistema.

 <b>STEEL SEGURIDAD PRIVADA LTDA.</b> <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b> NIT. 830.106.318-4 	<b>Versión: 01</b>
<b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b>	<b>MA-GQ-01</b>

- **Frecuencia de realización de copias de seguridad.**
- La realización de copias de seguridad ha de ejecutarse diariamente, éste es el principio que debe regir la planificación de las copias.
- **Mecanismos de comprobación**
- Se deben definir mecanismos de comprobación de las copias de seguridad, aunque los propios programas las efectúen, para verificar el estado de la copia, es conveniente planificar dentro de las tareas de seguridad la restauración de una parte de la copia o de la copia completa periódicamente cada 3 meses, como mecanismo de prueba y garantía.
- **Responsable del proceso**
- Se debe designar a una persona que incluya entre sus funciones la supervisión del proceso de copias de seguridad, el almacenamiento de los soportes empleados en un lugar designado a tal fin, e incluso de la verificación de que las copias se han realizado correctamente. Este rol será definido por el área administrativa de STEEL SEGURIDAD PRIVADA LTDA.
- El responsable del proceso deberá guardar las copias de seguridad en un lugar alejado, como, por ejemplo, una caja de seguridad o cualquier otro sitio asegurado contra incendios, para que, en caso de que se produzca algún desastre, los datos se encuentren protegidos. Además deberá formar equipos de evaluación (auditoria de cumplimiento de los procedimientos sobre Seguridad).
- Cada una de las sedes de STEEL, que almacene información que sirva para la operatividad de la organización, deberá designar un responsable de la seguridad en su área, pudiendo ser el jefe de dicha área operativa, Asistentes Administrativo u Operativo. Quienes entre sus responsabilidades y funciones de seguridad de la información tendrán:

 <b>STEEL SEGURIDAD PRIVADA LTDA.</b> <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b> NIT. 830.106.318-4 	<b>Versión: 01</b>
<b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b>	<b>MA-GQ-01</b>

- ✓ Ponerse en contacto con los miembros de su área para darles a conocer las políticas y procedimientos a seguir para la seguridad de la información.
- ✓ Proporcionar soporte técnico para las copias de respaldo de las fuentes de los servicios en desarrollo.
- ✓ Verificar el funcionamiento óptimo de los componentes de red.
- ✓ Establecer procedimientos de seguridad en los sitios de recuperación.
- ✓ Organizar la prueba de hardware y software.
- ✓ Ejecutar trabajos de recuperación.
- ✓ Participar en las pruebas y simulacros de desastres.
- ✓ Revisar que las Normas y procedimientos con respecto a Backups, seguridad de equipos y data se cumpla.
- ✓ Supervisar la realización periódica de los backups, por parte de los equipos operativos, comprobando físicamente su realización, adecuado registro y almacenamiento.
- ✓ Informar de los cumplimientos e incumplimientos de las Normas, para las acciones de corrección respectivas.

## 11.2 Actividades Durante el Desastre.


Una vez presentada la Contingencia o Siniestro, se deberán ejecutar las siguientes actividades, planificadas previamente:

### 11.2.1 Plan de emergencias

En este plan se establecen las acciones que se deben realizar cuando se presente un Siniestro, así como la difusión de las mismas.

Es conveniente prever los posibles escenarios de ocurrencia del Siniestro:

- Durante el día.
- Durante la Noche o madrugada.

	<p><b>STEEL SEGURIDAD PRIVADA LTDA.</b>  <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b>  NIT. 830.106.318-4</p> 	<p><b>Versión: 01</b></p>
<p><b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b></p>		<p><b>MA-GQ-01</b></p>

Este plan deberá incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre el siniestro, debiendo detallar:



- Vías de salida o escape.
- Plan de Evacuación del Personal. - Plan de puesta a buen recaudo de los activos (incluyendo los activos de Información) de la Institución (si las circunstancias del siniestro lo posibilitan).
- Ubicación y señalización de los elementos contra el siniestro (extintores, etc.)
- Secuencia de llamadas en caso de siniestro, tener a la mano: elementos de iluminación (linternas), lista de teléfonos de Bomberos / Ambulancia, Jefatura de Seguridad y de su personal (equipos de emergencia) nombrados para estos casos.

A continuación detallamos ciertas normas sugeridas para el caso que se presente un siniestro, sea este robo, sismo o incendio que son los más comunes:

✓ **Robos:**

El personal de STEEL Seguridad Privada Ltda con el fin de resguardar su integridad, deberá tener en cuenta las siguientes recomendaciones:

- Mantener la calma: No oponer resistencia, en especial si el criminal está armado o se nota que esté bajo el influjo de drogas.
- Inteligencia: Tratar de retener frases expresadas por el atacante y evitar mirarlo directo a los ojos para prevenir enfrentamientos.
- Memoria: Aprenderse el número de placas y características del automóvil en caso de que los agresores escapen en un vehículo.
- Sencillez: La gente debe evitar ser ostentosa y mantenerse atenta a lo que sucede a su alrededor.

	<p><b>STEEL SEGURIDAD PRIVADA LTDA.</b>  <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b>  NIT. 830.106.318-4</p> 	<p><b>Versión: 01</b></p>
<p><b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b></p>		<p><b>MA-GQ-01</b></p>


✓ **Sismos:**

Si el Sismo no es fuerte, tranquilícese, acabará pronto, si es fuerte, mantenga la calma, agudice la atención para evitar riesgos y recuerde las siguientes instrucciones:

- Si está dentro del edificio, quédese dentro, hasta poder salir calmadamente; si está fuera, permanezca fuera, buscando un área despejada.
- Dentro de un edificio busque estructuras fuertes: como por ejemplo una mesa, bajo el dintel de una puerta, junto a un pilar, pared maestra o en un rincón y proteja su cabeza.
- Apague todo fuego, con extintores. No utilice ningún tipo de llama (cerilla, encendedor, vela, etc.) durante o inmediatamente después del temblor.
- Fuera de un edificio, aléjese de cables eléctricos, cornisas, cristales, pretilas, etc.
- No se acerque ni penetre al edificio para evitar ser alcanzado por la caída de objetos peligrosos (cristales, cornisas, etc.) Vaya hacia lugares abiertos, no corra y cuidado con el tráfico.

✓ **Incendios:**


- Conserve la calma: No Grite, No Corra, No Empuje. Puede provocar un pánico generalizado. A veces este tipo de situaciones causan más muertes que el mismo incendio.
- Busque el extintor más cercano y trate de combatir el fuego. Si no sabe manejar el extintor, busque a alguien que pueda hacerlo por usted.

 <b>STEEL SEGURIDAD PRIVADA LTDA.</b> <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b> NIT. 830.106.318-4 	<b>Versión: 01</b>
<b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b>	<b>MA-GQ-01</b>

- Si el fuego es de origen eléctrico no intente apagarlo con agua.
- Cierre puertas y ventanas para evitar que el fuego se extienda, a menos que éstas sean sus únicas vías de escape.
- Al momento de abrir una puerta, verifique que la chapa no esté caliente antes de abrirla; si lo está, lo más probable es que haya fuego al otro lado de ella, no la abra.
- En caso de que el fuego obstruya las salidas, no se desespere y colóquese en el sitio más seguro. Espere a ser rescatado.
- Si hay humo colóquese lo más cerca posible del piso y desplácese "a gatas". Tápese la nariz y la boca con un trapo, de ser posible húmedo.
- Si se incendia su ropa, no corra: tírese al piso y ruede lentamente. De ser posible cúbrase con una manta para apagar el fuego.

#### 11.2.2 Formación de equipos.

Si bien la premisa básica es la protección de la Integridad del personal, en caso de que el siniestro lo permita (por estar en un inicio o estar en una área cercana, etc.), deberá de existir dos equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y otro para el salvamento de los recursos Informáticos, de acuerdo a los lineamientos o clasificación de prioridades, para salvar los equipos señalados en las actividades previas al desastre.

 <b>STEEL SEGURIDAD PRIVADA LTDA.</b> <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b> NIT. 830.106.318-4 	<b>Versión: 01</b>
<b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b>	<b>MA-GQ-01</b>

### 11.2.3 Entrenamiento.

Un aspecto importante es que el personal tome conciencia de que los siniestros (incendios, sismos, etc.) pueden realmente ocurrir, y tomen con seriedad y responsabilidad estos entrenamientos, para estos efectos es conveniente que participen los elementos directivos de Sudamericana de Software. Se llevará a cabo estos entrenamientos mediante la implementación de simulacros y charlas ante los posibles siniestros que pudiesen ocurrir en la empresa.

### 11.3 Actividades Después Del Desastre.

Después de ocurrido el Siniestro o Desastre es necesario realizar las actividades que se detallan en el Plan de contingencias establecido previo a su ejecución se deben tomar en cuenta los puntos que se detallan a continuación.

#### 11.3.1 Evaluación de daños.

Inmediatamente después que el siniestro ha concluido, se deberá evaluar la magnitud del daño que se ha producido, que sistemas se están afectando, que equipos han quedado no operativos, cuales se pueden recuperar, y en cuanto tiempo.


Para la evaluación de los daños se realizarán las preguntas o indagaciones necesarias por parte del equipo encargado de la vigilancia y/o supervisión del área en donde se produjo el siniestro.

El objetivo de establecer esta evaluación hace que los encargados de cada área puedan reconocer el tipo de desastre que se produjo sea este en el ámbito físico o lógico.

Cuando se obtengan los resultados de la evaluación realizada, el equipo encargado de la supervisión verificará en cuál de los puntos establecidos en el plan de contingencias encaja el siniestro.

Si se tratase de un desastre en el ámbito lógico se deben verificar los siguientes puntos:



 <b>STEEL SEGURIDAD PRIVADA LTDA.</b> <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b> NIT. 830.106.318-4 	<b>Versión: 01</b>
<b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b>	<b>MA-GQ-01</b>

- Para la información existente de STEEL SEGURIDAD PRIVADA LTDA se debe verificar la calidad e integridad de la misma (hacer las pruebas sobre los programas que antes del desastre funcionaban correctamente).
- La calidad e integridad de la información de respaldo.
- En lo posible volver al estado original de la información antes del desastre

Si se tratase de un desastre en el ámbito físico se deben verificar los siguientes puntos:

- Por una Suspensión o caída del suministro eléctrico, el estado del hardware (Equipos de cómputo, Equipos de telecomunicaciones).
- Si se trata de un siniestro de fuerza mayor como son: incendios, inundaciones, maremotos, tornados, robo a la empresa; se deben seguir los lineamientos establecidos en el plan de contingencias para desastres de gran magnitud.


### 11.3.2 Priorización de actividades del plan de acción.

Con la evaluación de daños reales y su comparación contra el Plan de acción, tendremos la lista de las actividades que debemos realizar, siempre priorizándola en vista a las actividades estratégicas y urgentes de nuestra Empresa.

Será muy importante el evaluar la dedicación del personal a las actividades que puedan no haberse afectado, para ver su asignación temporal a las actividades afectadas, en apoyo al personal de los sistemas afectados y soporte técnico.

### 11.3.3 Ejecución de actividades.

Para la ejecución de actividades previamente planificadas en el Plan de acción se definen los siguientes equipos de trabajo:

 <b>STEEL SEGURIDAD PRIVADA LTDA.</b> <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b> NIT. 830.106.318-4 	<b>Versión: 01</b>
<b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b>	<b>MA-GQ-01</b>

- Equipo de Salvaguarda de información.
- Equipo de Salvaguarda de hardware.
- Equipo de Salvaguarda de la empresa

Cada uno de estos equipos cuenta con un coordinador que deberá reportar diariamente el avance de los trabajos de recuperación y, en caso de producirse algún problema, reportarlo de inmediato a la jefatura a cargo del Plan de Contingencias.

Los trabajos de recuperación tendrán dos etapas, la primera la restauración del servicio usando los recursos de la Institución o local de respaldo, y la segunda etapa es volver a contar con los recursos en las cantidades y lugares propios del Sistema de Información, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar el buen servicio de nuestro Sistema e imagen Institucional, como para no perjudicar la operatividad de la Institución o local de respaldo.

#### **11.3.4 Evaluación de resultados.**

Una vez concluidas las labores de Recuperación del (los) Sistema(s) que fueron afectados por el siniestro, debemos de evaluar objetivamente, todas las actividades realizadas, que tan bien se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades del plan de acción y como se comportaron los equipos de trabajo.

De la Evaluación de resultados y del siniestro en sí, darán como resultado dos tipos de recomendaciones, una la retroalimentación del plan de Contingencias y otra una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionó el siniestro.

 <b>STEEL SEGURIDAD PRIVADA LTDA.</b> <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b> NIT. 830.106.318-4 	<b>Versión: 01</b>
<b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b>	<b>MA-GQ-01</b>

### 11.3.5 Retroalimentación del plan de acción.

Con la evaluación de resultados, debemos de optimizar el plan de acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente.

El otro elemento es evaluar cuál hubiera sido el costo de no haber tenido nuestra Institución el plan de contingencias llevado a cabo.

## 12 POLÍTICA DE SEGURIDAD INFORMÁTICA, DE LA INFORMACIÓN Y LOS DATOS.

### 12.1 Seguridad para los servicios informáticos

- **Alcance**


Los funcionarios de STEEL Seguridad Privada Ltda. Que tienen acceso a la red y a los servicios informáticos disponibles

- **Objetivo**

Proteger a la entidad del uso inadecuado de los medios electrónicos por parte de los funcionarios de STEEL Seguridad Privada Ltda. Así como protegerse de las amenazas propias de internet y que están al alcance de los usuarios.

- **Descripción**

El correo electrónico asignado a cada uno de los funcionarios de STEEL Seguridad Privada Ltda. y/o contratistas, deberán ser usados únicamente para las funciones asignadas a cada funcionario y para las actividades contratadas en caso de los contratistas. Los funcionarios deben abstenerse de utilizar este medio para actividades de índole personal y para la participación en foros y comunidades en las que actúen a título personal y no como funcionarios de STEEL Seguridad Privada Ltda.

	<p><b>STEEL SEGURIDAD PRIVADA LTDA.</b>  <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b>  NIT. 830.106.318-4</p> 	<p><b>Versión: 01</b></p>
<p><b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y  RECUPERACIÓN DE LOS DATOS.</b></p>		<p><b>MA-GQ-01</b></p>

En caso de que se requiera la participación en nombre de la empresa, sólo se podrá usar el correo institucional siempre y cuando exista una autorización del jefe inmediato.

La empresa se reserva el derecho de acceder y develar todos los mensajes enviados por este medio, para cualquier propósito. Para este efecto, el empleado aceptará estas condiciones de uso de los servicios disponibles. Las cuentas de correo electrónico se asignarán de manera individual a cada empleado y se identificará ya se con el nombre y apellido del empleado o con el cargo que ocupa dentro de la empresa.

El uso de Internet y de las facilidades disponibles a los empleados de STEEL Seguridad Privada Ltda. Se llevará a cabo en el marco de las políticas de uso de Internet, definidas por la empresa. La navegación en sitios no seguros de Internet, tales como sitios de descarga de música, videos, sitios para adultos, archivos ejecutables, entre otros y que atenten contra la seguridad de la red está prohibida.



La entidad dispondrá de un software para protección de virus, antivirus que garantiza la defensa ante amenazas de código malicioso que afecte el desempeño de los recursos informáticos con que cuenta la entidad. Es responsabilidad de los usuarios informar oportunamente acerca de una sospecha de infección por un virus, recepción de SPAM o comportamiento anómalo por causas desconocidas, a la persona encargada o designada por STEEL Seguridad Privada Ltda. ante estas situaciones de riesgo, deberá abstenerse de usar su computador y desconectarlo físicamente de la red.

- **Responsables**

Funcionarios de STEEL Seguridad Privada Ltda. Que tengan acceso a la red.

- **Sanciones**

El incumplimiento de esta política conllevará a la suspensión de la cuenta de acceso a la red, y de la notificación al superior inmediato, con copia al departamento de Gestión Humana.

 <b>STEEL SEGURIDAD PRIVADA LTDA.</b> <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b> NIT. 830.106.318-4 	<b>Versión: 01</b>
<b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b>	<b>MA-GQ-01</b>

## 12.2 Política de Seguridad física y del entorno.

- **Alcance**

Empleados de STEEL Seguridad Privada Ltda. que tienen acceso a la red y a los servicios informáticos disponibles y Personas usen recursos propios o dispongan recursos para el desarrollo de actividades en la empresa y que tengan acceso a la red y a los recursos o servicios informáticos disponibles

- **Objetivo**

Garantizar que el acceso físico a las instalaciones de operación de equipos de cómputo y de telecomunicaciones se realiza bajo medidas de seguridad que permitan que únicamente el personal autorizado pueda manipular o tener contacto con los equipos activos y sensibles para la operación.


- **Descripción**

La empresa deberá contar con los mecanismos de control de acceso tales como control al ingreso de personal ajeno a las instalaciones, los equipos de cómputo deberán tener claves de acceso controladas por el usuario y por la persona designada por la empresa, los equipos de telecomunicación deberán tener un control por los usuarios asignados.

Los visitantes de las oficinas de la empresa deben ser acompañados durante todo el tiempo por un empleado autorizado.

Todos los visitantes requieren un acompañante incluyendo clientes, antiguos empleados y miembros de la familia del trabajador.

Las áreas donde se encuentran equipos de cómputo, deben ser lugares de acceso restringido y cualquier persona que ingrese a ellos deberá registrar el motivo del ingreso y estar acompañada permanentemente por el personal que labora cotidianamente en estos lugares.

	<p><b>STEEL SEGURIDAD PRIVADA LTDA.</b>  <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b>  NIT. 830.106.318-4</p> 	<p><b>Versión: 01</b></p>
<p><b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b></p>		<p><b>MA-GQ-01</b></p>

Toda persona que se encuentre dentro de la entidad deberá portar su identificación en lugar visible.

Las centrales de conexión de red o centros de cableado deben ser catalogadas como zonas de alto riesgo, con limitación y control de acceso.

Todos los computadores portátiles son responsabilidad de cada usuario y el uso de los mismos fuera de las instalaciones de la compañía es responsabilidad de cada uno de sus usuarios.

Los equipos como computadores y/o servidores no deben moverse o reubicarse sin la aprobación previa de la persona encargada por la Empresa.

Los particulares en general, entre ellos, los familiares de los empleados, no están autorizados para utilizar los recursos informáticos de la empresa.

- **Responsables**

Funcionarios encargados por la empresa, contratistas y sus jefes inmediatos.

- **Sanciones**



El incumplimiento de esta política conllevará a notificación al jefe inmediato, con copia al departamento de Gestión Humana.

### 12.3 Política Acceso a la información

- **Alcance**

Empleados de STEEL Seguridad Privada Ltda que tienen acceso a la red y a los servicios informáticos disponibles.



 <b>STEEL SEGURIDAD PRIVADA LTDA.</b> <b>SU SEGURIDAD ES NUESTRO COMPROMISO</b> NIT. 830.106.318-4 	<b>Versión: 01</b>
<b>MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.</b>	<b>MA-GQ-01</b>

- **Objetivo**

Garantizar que la información, sea dispuesta a los funcionarios, de manera que se pueda utilizar efectivamente, de manera segura y sin afectación a la calidad y confiabilidad de la misma.

- **Descripción**

Todos los empleados de STEEL Seguridad Privada Ltda, deberán tener acceso sólo a la información necesaria para el desarrollo de sus actividades, En el caso de terceros externos a la compañía, deberán contar con una solicitud de autorización.

El otorgamiento de acceso a la información está regulado mediante las normas y procedimientos definidos para tal fin.

Los contratistas, proveedores o terceras personas solamente deben tener permisos durante el periodo del tiempo requerido para llevar a cabo las funciones convenidas y aprobadas.

- **Responsables**

Todos los empleados de STEEL Seguridad Privada Ltda y contratistas y sus jefes inmediatos.

- **Sanciones**

El incumplimiento de esta política conllevará a notificación al jefe inmediato, con copia al departamento de Gestión Humana.



# STEEL SEGURIDAD PRIVADA LTDA.

SU SEGURIDAD ES NUESTRO COMPROMISO

NIT. 830.106.318-4



Versión: 01

## MANUAL DE SEGURIDAD INFORMÁTICA, PROTECCIÓN Y RECUPERACIÓN DE LOS DATOS.

MA-GQ-01

REVISADO POR:	APROBADO POR:	FECHA:
Subgerente - Gerente	Junta Directiva	ago-15

COPIA CONTROLADA

ESTAMOS CONTRIBUYENDO CON LA CONSERVACION DEL MEDIO AMBIENTE

Fecha de Edición o Actualización Dic.- 2016

Proceso: Sistemas de Gestión Integrado