Manual de Estándares de Seguridad de La Información

Preparado por:	Revisado por:	Aprobado por:
Robert Jimenez	Humberto Sánchez	. Miguel Montoya

Presentación y propósito

Este manual lleva como nombre ***Manual de Estándares de Seguridad de Información***,, en su elaboración se ha considerado plasmar la caracterización de lo que es el proceso de manejo de los estándares de seguridad de información de todos nuestros productos /servicios.

Tiene como finalidad describir en cada caso cual es el procedimiento a seguir de acuerdo al tipo y grado de seguridad de información responsabilidad de la empresa. Esta dirigido al personal de la empresa, clientes y terceras partes que requieran información formal con relación a las características de cómo ***INCALL*** maneja la seguridad de la información***.***

El original del Manual se guarda en la Dirección de Administración, se distribuyen copias controladas al Director General y Gerentes, de acuerdo con el procedimiento para la Distribución y Custodia de Manuales y Documentos del Sistema de la Calidad de ***INCALL.*** El desarrollo, implantación y mantenimiento de éste documento es responsabilidad de la Dirección de Procesos y Calidad. Las disposiciones y normativas establecidas son de obligatorio cumplimiento, tiene vigencia a partir de 12 de Diciembre, 2017 fecha de su última revisión.

Se establece a partir de esta fecha revisiones anuales de este instrumento.

1. Generalidades

1.1 Objetivo.

La aplicación y cumplimiento de Los Estándares de Seguridad de Información de ***INCALL*** servirán de marco para el manejo efectivo de la Información inherentes a sus procesos internos y a la protección de los datos suministrados por sus clientes para .

Los Estándares de Seguridad de Información de ***INCALL*** definen los resultados que se deben alcanzar en el manejo de los datos y cada área manejara procesos que definan como se van a cumplir.

Para el cumplimiento de los Estándares de Seguridad de Información se definirán las políticas, y adicionalmente los responsables para velar por el cumplimiento de los mismos.

Estos estándares definen categorías tanto para la clasificación de la información como para la clasificación de la seguridad de la infraestructura ya que el control que se debe mantener sobre los datos no sólo depende del nivel crítico de la información sino también del ambiente en los medios de almacenamiento, proceso y transmisión.

Adicionalmente la aplicación de estos estándares permitirá determinar y controlar las probabilidades de amenazas, detectar ataques, los mecanismos de protección

Para asegurar eficazmente la información que ***INCALL*** maneja se debe conocer en todo momento los controles para garantizar la confidencialidad, los usuarios de los servicios, la disponibilidad de los datos, como reducir los problemas o las situaciones de ataques.

1.2 Alcances y Cumplimiento.

Todas las áreas, departamentos y oficinas regionales de ***INCALL*** deberán aplicar estos estándares como requisitos mínimos para garantizar la seguridad de la información.

Toda la organización de ***INCALL*** debe asegurar que sus empleados y proveedores externos cumplan con los Estándares de Seguridad de la Información que apliquen a sus áreas mediante la aplicación de los procedimientos establecidos para tal fin.

El Gerente y Coordinador de cada área es responsable de garantizar el cumplimiento de los estándares a través de la implementación de los procesos y procedimientos que cumplan con los requisitos.

Si un área no cumple con uno o más de los requisitos detallados en estos estándares, éstos se deben registrar y documentar usando el formulario de Riesgo Informacional (ver punto 10.4), donde se especifica la justificación y los riesgos relacionados. El no cumplimiento debe estar reportado y aprobado por el responsable asignado en cada área.

En el caso de incumplimiento de los estándares adicionalmente se debe remitir copias de los formularios aprobados de Riesgo al responsable de Seguridad de la información de ***INCALL***, al propietario de estos estándares y a la Gerencia General.

Las excepciones solo serán autorizadas por la directiva y las acciones correctivas se implementaran una vez analizado cada caso y será responsabilidad de las áreas involucradas ejecutar las acciones correctivas.

Las personas autorizadas para el cumplimiento de esta normativa son los Directores – Gerentes y los Gerentes de cada área en ejecutarla (ver anexo I).

1.3 Responsable.

Las políticas son definidas por la directiva de ***INCALL*** quienes serán los propietarios de las mismas y definirán los responsables de su cumplimiento

El responsable del cumplimiento, auditoría, actualización y custodio de los estándares de Seguridad de Información es el Administrador de Seguridad de Información. El administrador de Redes será el responsable por la implementación de las políticas y estándares. Las consultas o inquietudes que surjan de la interpretación de estos estándares las debe abordar el grupo de tecnología de seguridad de la información.

1.4 Propiedad de la Información.

Dentro de cada área de la organización de ***INCALL*** se nombraran los propietarios de la información por escrito, y los mismos clasificarán la información de ***INCALL*** según las clasificaciones de la información: Pública, Interna, Restringida, Confidencial y Altamente confidencial

Para cada área de la organización se identificará:

a) El nivel crítico de cada sistema o proceso de información relacionados con la seguridad de datos

b) Las instancias donde el sistema o proceso no cumple con los estándares de seguridad de datos.

c) Los aspectos críticos del personal, tecnología y procedimientos que podrían causar que el sistema o proceso de información se alterara o afectara.

d) Los escenarios de amenaza con base a las vulnerabilidades o aspectos críticos.

e) Los aspectos de no cumplimiento para documentar los diferentes riesgos

f) Los planes de acción de seguridad para mitigar el riesgo relacionado con instancias de no cumplimiento o con sistemas de procesos de información identificados como riesgo alto o medio.

g) El cumplimiento de los procesos y el uso de los formularios para la gestión del riesgo de la seguridad de la información que sean especificados

h) La evaluación por área del nivel de seguridad necesario para proteger esta información y garantizar que se manejen los controles para alcanzar el nivel especificado.

i) Mantenimiento de los inventarios de todos los sistemas y procesos de información por área donde se especifique al propietario de la información bajo su control, la clasificación de la información, el nivel crítico, el nivel de riesgo y la clasificación de seguridad de la infraestructura.

2. Bases para el establecimiento de Estándares

Para poder aplicar los Estándares de Seguridad de Información debemos definir que la Información de ***INCALL*** se refiere al registro de información de clientes, transacciones, memos, mails, software, datos de entrada y procesados y todos aquellos datos creados por la organización durante el funcionamiento de la empresa.

Para todos los efectos de estándares de seguridad de la información se basaran en los siguientes aspectos:

2.1 Clasificación de la Información.

a) ***Pública:*** Información que está libremente disponible dentro y fuera de la organización de ***INCALL***y puede ser usada por el público sin autorización del propietario de la información.

b) ***Interna:*** Información que puede ser compartida dentro de la organización de ***INCALL***, no debe divulgarse fuera de ***INCALL***y no está clasificada como restringida, altamente confidencial o confidencial.

c) ***Confidencial:*** Información que ***INCALL*** esta obligada a proteger y no divulgar con respecto a clientes, empleados y negocios. Si esta información es divulgada por personas no autorizadas puede tener un impacto sobre las ventajas competitivas del negocio.

d) ***Altamente Confidencial****:* Información que, si se divulga a individuos no autorizados, podría tener un impacto significativo en las obligaciones legales o reglamentarias de ***INCALL*** o en su condición financiera, clientes o franquicia.

e) ***Restringida:*** Información que, no puede ser divulgada a personas que no estén autorizadas, ya que podría tener un impacto en obligaciones legales, en aspectos financieros o en la relación contractual con los clientes de ***INCALL*** generando pérdidas muy significativas tanto económica como de imagen y continuidad operativa.

2.2 Requisitos de Encriptación.

Con el fin de determinar si se requiere una encriptación de los datos de ***INCALL***, primero identifique la clasificación de la seguridad de la infraestructura del ambiente en el cual los datos se van a almacenar o transmitir y luego aplique los siguientes requisitos:

a) ***Información Pública e Interna:*** No hay requisito de encriptar esta información.

b) Información Altamente Confidencial:

- ***Transmisión:*** La información altamente confidencial se debe encriptar, excepto cuando se transmita mediante una infraestructura de clase A+.

- **Almacenamiento:** Se debe encriptar la información altamente confidencial, excepto cuando se almacene en una infraestructura clase A o A+.

c) ***Información Restringida:*** La información restringida se debe encriptar, excepto cuando se almacene o transmita en una infraestructura clase A+. Los datos de autenticación se deben encriptar en todos los ambientes excepto para usos de una sola vez, contraseñas dinámicas o PRE-vencidas o llaves públicas.

2.3 Clasificación de la Seguridad de la Infraestructura.

La infraestructura de ***INCALL*** se clasificará de la siguiente manera:

a) ***No Clasificada:*** La infraestructura no administrada por ***INCALL***o sus agentes contratados, incluyendo la Internet, se considerará como una estructura no clasificada y considerada como un ambiente hostil.

b) ***Clase A+:*** La infraestructura de clase A+ también estará diseñada para proteger contra amenazas de entidades, incluyendo aquellas con acceso a la red interna, donde el ataque requiere de individuos que posean altos niveles de sofisticación técnica y conocimiento de operaciones internas técnicas o del negocio y donde al menos una de las entidades se le ha concedido acceso privilegiado.

c) ***Clase A:*** La infraestructura de clase A también estará diseñada para protegerse contra amenazas de entidades, incluyendo aquellas con acceso a la red interna, donde el ataque requiere que los individuos posean altos niveles de sofisticación técnica y conocimiento de las operaciones internas técnicas o del negocio.

d) ***Clase B:*** La infraestructura de clase B también estará diseñada para protegerse contra amenazas de entidades, incluyendo aquellas con acceso a la red interna, donde el ataque requiere que los individuos posean altos niveles de sofisticación técnica.

e) ***Clase C:*** La infraestructura de clase C también estará diseñada para proteger contra las amenazas de entidades, incluyendo aquellas con acceso a la red interna, donde el ataque se puede lograr a través de un “usuario casual” utilizando utilerías y herramientas de penetración.

f) ***Clase D:*** La infraestructura de clase D tiene controles mínimos de acceso con la intención de permitir acceso por parte de los empleados de ***INCALL***y proveedores externos.

2.4 Datos de Autenticación.

Con base en estos criterios, la siguiente tabla demuestra cuando se requiere de encriptación para la transmisión o almacenamiento de información de ***INCALL***:

Clasificación de la Información	***Clasificación de la Seguridad de la Infraestructura***					
	No Clasificada	Clase D	Clase C	Clase B	Clase A	Clase A+
Datos de Autenticación	Si	Si	Si	Si	Si	Si
Restringida	Si	Si	Si	Si	Si	No
Altamente Confidencial	Si	Si	Si	Si	Si Tránsito No Almacenamiento	No
Confidencial	Si	Si	No	No	No	No
Interna	No	No	No	No	No	No
Pública	No	No	No	No	No	No

a) ***No clasificada:*** Se refiere a infraestructura no administrada por ***INCALL*** o su agente contratado, incluyendo la Internet, y se tratará como hostil.

b) ***Almacenamiento:*** Se refiere a cualquier medio de almacenamiento electrónico, magnético u óptico.

c) ***Contraseñas:*** Las contraseñas estáticas no se deben encriptar cuando:

- Se usen para tener acceso a un sistema de información.

- Se usen para tener acceso a información a través de una infraestructura de clase C o mayor, donde el nivel crítico de la integridad o disponibilidad de la información es baja.
- Se usen para tener acceso a la información a través de una infraestructura de clase C o mayor donde existan controles mitigantes adecuados para la integridad y disponibilidad de la información.

Si la encriptación requerida no se puede lograr o no sea práctica, el negocio debe implementar controles adicionales para la infraestructura de ***INCALL*** para aumentar la clasificación de seguridad de la infraestructura a un nivel al cual no se requiera encriptación.

3. Estándares de Seguridad de la Información

3.1 Identificación y Autenticación.

a) Todas las plataformas de tecnología de ***INCALL*** autenticarán la identidad de los usuarios antes de iniciar una sesión o transacción, a menos que el usuario tenga derecho únicamente a leer datos INTERNOS o PÚBLICOS en estas plataformas.

b) Todos los usuarios serán identificados en la plataforma de tecnología mediante un(a):
   - Login: está formado por la iniciar del Nombre seguido del Apellido. En el caso que haya dos empleado con el mismo Nombre y Apellido, se utilizara la inicial del segundo Nombre o Segundo Apellido.
   - Método de autenticación que permita la identificación única del usuario, una contraseña dinámica que tendrá las siguientes características:
   - Se almacena usando cifrado reversible
   - Longitud mínima de 8 caracteres que sea alfanumérico y caracteres especiales
   - Duración mínima de 1 día y máxima de 20 de días

c) Los usuarios son responsables por toda la actividad relacionada con su identificación del usuario y contraseña.

d) Todos los usuarios serán identificados la plataforma Web a través de una identificación única del usuario, Compuesta por la inicial del nombre seguida de un punto y el apellido más el carácter especial @ seguida del identificador del dominio, en este caso sería. Ejemplo: r.jimenez@incallsudamerica.com

e) Las contraseñas:

- Nunca se deben compartir, hacerse públicas o escribirse.
- Nunca deben aparecer en la pantalla en texto claro (con la excepción de reinicializaciones (reset) de contraseña para un solo uso).

f) Las identificaciones de usuarios relacionadas con una contraseña se deben invalidar después de un máximo de cinco (5) intentos fallidos de conexión.

g) Se implementará un proceso documentado para garantizar que todas las contraseñas se cambien periódicamente y que las identificaciones de usuarios se invaliden después de un período establecido de inactividad. Los periodos seleccionados dependerán de la importancia del sistema de información. Es posible ignorar el requisito de cambiar las contraseñas los sistemas de información, siempre y cuando se les recuerde periódicamente al personal que el cambio manual de sus contraseñas brinda mayor seguridad.

h) Se usarán contraseñas dinámicas o certificados digitales para el acceso remoto de clientes a la red global de ***INCALL*** y para el acceso de administradores a enrutadores y firewalls.

i) Los sistemas de información que usan contraseñas dinámicas o certificados digitales usarán los servicios de autenticación aprobados por el administrador de seguridad para validar la contraseña o el certificado.

3.1.1 Proceso De Actualización de Contraseñas.

a) Persona Responsable: Administrador de Seguridad de Información

b) En el caso de que la cuenta sea bloqueada por error del usuario o por no recordar su clave, este usuario o empleado deberá comunicarse con el administrador de seguridad de información para la verificación de lo sucedido y su posterior actualización.

c) La Persona responsable de la seguridad de la información velará por el cumplimiento de las políticas de actualización de contraseñas y por la revisión periódica y mantenimientos de los parámetros definidos en el Dominio INCALL sobre la plataforma Windows 2012 Server.

Parámetros definidos en el Servidor de Dominio.

- Directivas de Seguridad de Contraseñas
- Almacenar contraseñas usando cifrado reversible habilitada.
- Forzar el historial de contraseñas recordadas a un total de 5.

- Las contraseñas deben cumplir los requerimientos de complejidad (habilitada)
- Longitud mínima de la contraseña de (8) caracteres alfanuméricos
- Vigencia mínima de la contraseña (1) Día
- Vigencia máxima de la contraseña (20) Día

3.1.2 Ausencias de Personal.

a) En el caso de salidas o ausencias del personal, el Dpto. de Recursos Humanos o el departamento donde laboro, se notificará por mail a la Persona responsable de Seguridad de Información para que sea deshabilitada la cuenta del empleado, según los siguientes casos:

Ausencias Programadas o Temporales.

- **Vacaciones:** La cuenta se deshabilita temporalmente, por el tiempo que dure el empleado de vacaciones.
- **Reposo:** La Cuenta se deshabilita temporalmente, por el tiempo que dure de reposo el empleado.
- **Permiso Remunerados o no Remunerados:** La cuenta se deshabilita por el tiempo que dure de permiso.

Ausencias Definitivas.

- **Despido:** Se precederá a eliminar, después de la notificación de recursos humanos o del departamento donde laboro.
- **Renuncia:** Se precederá a eliminar, después de la notificación de recursos humanos o del departamento donde laboro.
- **Muerte:** Se precederá a eliminar, después de la notificación de recursos humanos o del departamento donde laboro.

3.1.3 Divulgación de las políticas de Actualización de Contraseñas.

a) Se realizará a través del documento que se le entrega al empleado cuando ingresa a la empresa.

b) Se realizará en el envío de e-mails mensuales, mediante una planilla predefinida.

c) Se realizará un documento breve con información el cual será publicado en la cartelera.

3.2 Autorización y Control de Acceso.

a) Todas las áreas implementarán controles de acceso que:

- Estén completamente documentados.
- Sean auditables.
- Garanticen que los usuarios reciban únicamente aquellos privilegios y autorizaciones necesarios para realizar su función.

b) En aquellas áreas donde los controles de acceso no sean posibles o estén prohibidos, se pueden implementar controles mediante el uso de pistas de auditoría.

c) Se protegerán todos los sistemas y procesos de información del acceso no autorizado y usando productos, funciones o procesos de seguridad dependiendo del nivel crítico del sistema o proceso de información, la clasificación de la información y la clasificación de seguridad de la infraestructura. Este requisito incluye ambientes de no producción como sistemas para pruebas y desarrollo.

d) Las autorizaciones de acceso se deben poder rastrear hasta la identificación del usuario y propietario asignado.

e) Se implementará un proceso documentado para revisar y verificar las autorizaciones de usuarios al menos semestralmente.

f) Se documentará e implementará un proceso para garantizar que los derechos de acceso reflejen los cambios en el estado del empleado y proveedor externo.

- Cada gerente será responsable por los derechos de acceso de los empleados y proveedores externos bajo su control. Los cambios requeridos a los derechos de acceso emitidos debido a traslados y cambios en las funciones del cargo se comunicaran formalmente vía mail a la función de administración de seguridad dentro de 24 horas. La comunicación identificará los derechos de acceso que se deben enmendar y la fecha real cuando se deben enmendar.
- Los gerentes deben notificar al administrador de seguridad vía mail dentro de 24 horas la sesión de empleados o proveedores externos que ya no trabajan para ***INCALL***.
- El Administrador de Seguridad notificará al Administrador de Redes vía mail los cambios de los derechos de acceso dentro de 7 días de la solicitud de un cambio.

- La notificación a la función de administrador de Seguridad y los cambios posteriores en los derechos de acceso se debe completar antes de que el empleado o proveedor externo sea notificado del cambio en el estado.

g) El texto de entrada aprobado por el departamento de seguridad, cuando sea compatible con el sistema operativo o aplicación, se presentara en todos los puntos de entrada al sistema donde un usuario inicialmente se conecta.

h) El acceso remoto a los sistemas de información estará protegido del uso no autorizado. En particular, todo acceso remoto está prohibido en cualquier sistema de información conectado a la red global de ***INCALL.***

i) La información confidencial, altamente confidencial y restringida sólo se debe almacenar en dispositivos de propiedad y administrados por ***INCALL*** o en dispositivos de propiedad de proveedores que están sujetos a un contrato que cumple con las políticas y estándares de ***INCALL***.

j) A menos que se apruebe por escrito por parte de administrador de seguridad se indica lo siguiente:

- Las redes de área local inalámbricas (WLAN's) y otros dispositivos inalámbricos están totalmente prohibidas en la red global de ***INCALL***.
- Los empleados no tendrán acceso a cuentas externas de email por Internet a través de la red global de ***INCALL***.

k) Como parte de su programa periódico de concientización sobre la seguridad de la información entre los empleados, se verificará que sus empleados conozcan que:

- La infraestructura de red de ***INCALL*** y el departamento de Seguridad de la Información, no permiten el uso de dispositivos Wireless de ningún tipo tales como: Router Wireless, Access Point, Tarjetas de Red Wireless.
- El área de soporte certificará que los equipos adquiridos, no incluyan en sus piezas tarjetas de red inalámbrica.

l) Las conexiones inactivas se desconectaran según los siguientes criterios:

- 24 horas después de la notificación formal del área si la conexión es en un área del acceso al público.
- 7 días después de la notificación formal para conexiones que no están asignadas a ningún individuo y que están localizadas en oficinas sin llaves, áreas comunes, salones de conferencia y otras áreas donde no se limita el acceso.
- 30 días después de la notificación para cualquier conexión asignada a una persona específica.

3.3 Confidencialidad e Integridad.

a) Se informarán a todos los usuarios de los sistemas o procesos de información (en particular a usuarios de e-mail y correo de voz) que toda la información almacenada, transmitida o manejada por estos sistemas o procesos es de propiedad de ***INCALL*** y que esta información puede ser revisada y supervisada para fines administrativos, de seguridad y otros propósitos legales.

b) Las áreas protegerán la información de ***INCALL*** sin importar el medio en el cual se encuentre.

c) Sujeto a las exclusiones especificadas en el punto de requisitos de encriptación, toda la información de ***INCALL*** que se almacene o transmita en un formato electrónico será encriptada. Si no se requiere encriptación, de todas maneras se debe proteger la información de ***INCALL*** de un acceso no autorizado.

d) Cada unidad de negocios desarrollará, documentará y exigirá un programa de escritorio limpio que proteja toda la información *restringida, altamente confidencial y confidencial* almacenada en cualquier medio contra un uso no autorizado.

e) La información *restringida, altamente confidencial y confidencial* en el punto en el cual la información ya no es útil para el negocio más cualquier período adicional de retención exigido por ley regulación o contrato será destruida de una manera proporcional al nivel de amenaza de la información.

f) El Administrador de Redes instalará, actualizará y mantendrá los productos antivirus aprobados por el administrador de seguridad en todos los computadores personales y en todos los servidores LAN, servidores de correo y otros dispositivos que almacenan contenido recibido de fuentes externas. La revisión para la instalación de los antivirus o revisiones de parches de los mismos, sería diaria ya que se generan versiones continuas. El Administrador de Seguridad de datos definirá cuales versiones serían instaladas y en donde antes de su instalación realizará pruebas y certificará las mismas para garantizar que las actualizaciones no afecten el ambiente de producción.

Las áreas autorizadas de Tecnología y Seguridad de Información:

- Sólo ejecutarán sistemas operativos y software que tengan el soporte de un proveedor externo o que tenga una publicación activa y apropiada de

revisiones (parches) y actualizaciones de configuración disponibles para abordar los problemas de seguridad.

- Aplicarán todas las revisiones (parches) de seguridad y configuraciones aprobadas dentro de los períodos de tiempo especificados por el proceso de gestión de amenaza de vulnerabilidad. Para los sistemas operativos se aplicaran los parches continuamente, el Administrador de Seguridad definirá cuales serán aplicados una vez revisados.

3.4 Detección de incidentes y respuesta.

a) El área de Tecnología junto con el Administrador de Seguridad y el Administrador de Redes de la información, desarrollará, documentará y garantizará el cumplimiento de los estándares.

b) El área de Tecnología junto con el Administrador de Seguridad verificarán que todos los sistemas de información que almacenan información de ***INCALL*** usen pistas de auditoría para registrar y reportar todos los intentos de violaciones de la seguridad del sistema y todos los eventos significativos relacionados con la administración de seguridad y de los sistemas, las transacciones financieras y la información del cliente.

c) El nivel de informes de las pistas de auditoría será proporcional a la criticidad del sistema de información.

d) El Administrador de Seguridad verificara que las pistas de auditoría sean generadas y realizara revisiones periódicas en proporción al nivel crítico del sistema de información. Se deberá actuar ante cualquier actividad sospechosa. El proceso de revisión se debe segregar para garantizar que los revisores no revisen su propia actividad.

3.5 Administración.

a) El Administrador de Seguridad y el Administrador de Redes verificarán que se realicen revisiones apropiadas de antecedentes y referencia a todo el personal de ***INCALL***(es decir, solicitantes de trabajo que han aceptado una oferta de trabajo y proveedores externos) que realizan funciones relacionadas con la seguridad a quienes se les conceda acceso altamente privilegiado (por ejemplo, administración del sistema, administración de la base de datos, control de cambios o estado de supervisor) a la información de ***INCALL***.

b) El Administrador de Seguridad y el Administrador de Redes incorporarán un proceso de revisión de seguridad de la información en los procesos y procedimientos para la selección, desarrollo e implementación de aplicaciones,

productos y servicios con el fin de garantizar el cumplimiento con estos estándares.

c) Cualquier individuo asignado a la función de administración de la seguridad de la información no debe realizar transacciones que entren en conflicto con esta función. Específicamente, no deben iniciar, programar, procesar o autorizar transacciones del negocio.

d) El Administrador de Seguridad y el Administrador de Redes implementarán un proceso para garantizar que todas las funciones, productos herramientas y servicios de seguridad se configuren para cumplir con estos estándares y que se retiren, invaliden o protejan todas las capacidades de acceso predeterminado para evitar su uso no autorizado.

e) Al menos anualmente, la junta directiva junto con el área de Seguridad de la información revisarán las prácticas y procedimientos de seguridad de la información. La revisión evaluará la idoneidad de estas prácticas y procedimientos con base en los cambios en sus procesos, tecnología, responsabilidades del negocio, la sensibilidad de la información del cliente o corporativa los riesgos que pueden amenazar esta información.

3.6 Entrenamiento y Concientización.

a) La Gerencia de Talento Humano coordinara con el Administrador de Seguridad de Información que todos los empleados, contratistas y personal temporal que sean nuevos para ***INCALL*** o que tengan un cambio significativo en la responsabilidad del cargo, reciban entrenamiento sobre los aspectos de su función relacionados con la seguridad de la información dentro de un plazo de 90 días después de su fecha de contratación.

b) La Gerencia de Talento Humano y el Administrador de Seguridad de Información verificará que todos los empleados, contratistas y personal temporal asistan anualmente a un programa de entrenamiento sobre seguridad de la información.

c) El administrador de seguridad de información verificara que los administradores de sistemas y administradores de seguridad y administrador de rede que manejan o apoyan los sistemas de información de ***INCALL***, reciban un curso de entrenamiento, al menos cada 6 meses.

d) La Gerencia de Talento Humano y el administrador de Seguridad de información verificarán que todos los empleados, contratistas y personal temporal anualmente reciba material sobre concientización respecto a temas relacionados con la seguridad de la información para su función.

3.7 Evaluación de Vulnerabilidades.

a) El Administrador de Seguridad de la Información y el administrador de redes verificarán que todos los productos, servicios o aplicaciones de ***INCALL***, que usan la Internet para conectividad o comunicaciones: Se sometan a una prueba de hacking ético independiente antes de que la aplicación o el sistema entre en producción o se sometan a una evaluación de la vulnerabilidad usando procesos de prueba de seguridad cada vez que se introduzcan actualizaciones en el ambiente de producción.

b) Todas las aplicaciones de Internet de nivel crítico mediano y bajo recibirán una evaluación anual de vulnerabilidad.

c) Los gerentes de infraestructura de tecnología verificarán que se realice una evaluación anual de vulnerabilidad de su infraestructura técnica.

d) El Administrador de Seguridad de la Información realizará trimestralmente la Revisión de la Configuración de Firewall y Equipos de Red y procederá a realizar un informe a la directiva con las observaciones detectadas y de no tener incidencias será aprobado por la misma.

4. Estándares de Uso

4.1 Firewalls y Sistemas de Detección de Intrusos.

a) El Administrador de Redes internas de ***INCALL*** verificará que: todas las conexiones externas de Protocolos de Internet (IP) hacia la red global de ***INCALL*** estén protegidas por un firewall y que todas las conexiones externas

de Internet a la red global de ***INCALL*** sean supervisadas por un sistema de detección de intrusos en tiempo real.

b) Únicamente se pueden usar firewalls, sistemas de detección de intrusos y proveedores de servicios de seguridad aprobados por el Administrador de Seguridad de información.

c) Todos los cambios de configuración a los firewalls y sistemas deben ser ejecutados por el Administrador de Redes en función de los lineamientos documentados del Administrador de Seguridad de datos y se deben registrar y archivar a diario.

d) El administrador de redes configurará los firewalls con una regla predeterminada de negar todo según los lineamientos del administrador de seguridad de información que verificara la configuración.

e) El Administrador de Seguridad de datos debe revisar los log de firewalls para detectar cualquier incidencia y cuando ocurran eventos sospechosos de seguridad, se debe documentar y realizar las notificaciones y escalamientos.

f) Todas las alarmas de los sistemas relacionadas con un firewall o un evento de seguridad se deben registrar y archivar a diario.

g) Los firewalls de ***INCALL*** y la administración de sistemas de detección de intrusos deben tener capacidad de responder a un evento de seguridad dentro de los 15 minutos después de su ocurrencia, 24horas al día, 7 días a la semana.

5. Procesos

5.1 Proceso de Manejo de Incidencias de Seguridad.

Incidente de Seguridad de la información:

Un incidente de seguridad de la información se define como:

a) Cualquier intento o violación consumada a la seguridad de los recursos informáticos.
b) Cualquier comportamiento que represente una amenaza potencial a la integridad, confidencialidad, o disponibilidad de la información de la empresa, sin importar el medio (electrónico, óptico, magnético, documentos, etc.) en que se encuentre.
c) Uso no autorizado de recursos informáticos de la empresa.

Un incidente puede ser ocasionado accidental o intencionalmente, a continuación se da una lista no limitativa de incidentes:

a) Mal uso de información de la empresa, no importando el medio que se utilice.

b) Acceso no autorizado a información de la empresa, no importando el medio que se utilice.

c) Modificación no autorizada de información, no importando el medio en que se encuentre.

d) Compartir Password

e) Intrusiones a equipo de computo o comunicaciones

f) Ataques de negación de servicio o degradación de sistemas

g) Destrucción no autorizada de información, no importando el medio en que se encuentre.

h) Actividades sospechosas, como por ej. Personas accesando información o equipos de cómputo y/o comunicaciones que no tienen relación con sus funciones, etc.

i) Mal uso de recursos, esta clase de incidentes contempla pero no se limita a:
    a. Envió de mails, impropios, ofensivos, cadenas, etc.
    b. Acceso a sitios impropios en Internet, por ej. chats, pornográficos, de hackers, etc.
    c. Publicar información de la empresa en Internet o en cualquier otro medio que pueda dañar la imagen o causar alguna afectación a la organización.

d. Uso de recursos informáticos de la empresa para propósitos diferentes a los objetivos del Negocio.

Los fraudes por Internet o correo electrónico (comúnmente llamados “Phishing”), así como los virus, son incidentes independientes. Los empleados deben reportar estos casos al jefe inmediato. La recepción de e-mail tipo SPAM, normalmente no es considerado un incidente de seguridad de la información, a menos que se presenten de manera masiva.

Los *virus/worm* no son normalmente considerados incidentes de seguridad de la información, todas las afectaciones o detecciones de *virus/worm* deben ser reportados al área de Sistemas. Si el reporte de virus/worm es masivo el área de Sistemas notificara al Administrador de Seguridad de la Información, quien evaluará y determinará si se debe levantar un reporte.

Equipo de respuesta a incidentes de seguridad (Seguridad de la Información):

Con la finalidad de atender los Incidentes de Seguridad a la Información que se detecten en la empresa, se define a un grupo de personas que conforman la Coordinación de Soporte y Seguridad de la Información quienes analizarán los incidentes de seguridad que se presentan en la empresa, identificando sus causas y definiendo soluciones para prevenir su ocurrencia; enfocándose en establecer ¿Que sucedió? ¿Cómo sucedió? y ¿Que se puede hacer para evitar que ocurra de nuevo? Este grupo tiene por objetivo manejar de forma adecuada los incidentes de seguridad de la información y se encuentra conformado por la coordinación de seguridad de datos y el área de soporte, a continuación el cuadro que se establecerá con la información correspondiente a los responsables y sus actividades: (ver anexo II)

Responsable de la Coordinación de Soporte y Seguridad de la Información	Nombre:	
	Teléfono en oficina Teléfono Movil e-Mail	
Grupo de trabajo de la Coordinación	Nombre:	
	Teléfono en oficina	

de Soporte, Seguridad de la Información y Administración de Redes	Teléfono Movil e-Mail	
Coordinación de Soporte, Seguridad de la Información y Administración de Redes	Las siguientes áreas (no es limitativo) pueden ser llamadas por el Responsable de la Coordinación de Soporte y Seguridad de la Información a formar parte del Equipo de Soporte y Seguridad dependiendo de la naturaleza y severidad del incidente: a. Supervisores b. Gerentes c. Coordinadores d. Sistemas e. Recursos Humanos. f. Jurídico. g. Dirección General	

Responsabilidades

Nombre del área / puesto	Descripción de su función dentro del procedimiento
Responsable de la **Coordinación de Soporte, Seguridad de la Información y Administración de Redes**	• Responsable de la adecuada coordinación y seguimiento de los incidentes de seguridad de la información que se reportan.
Grupo de trabajo de la Coordinación de Soporte, Seguridad de la Información y Administración de Redes	• Apoya al Responsable de la Coordinación de Soporte y Seguridad de la Información en la realización de todas sus funciones • Coordina el análisis, planteamiento de acciones correctivas y seguimiento de los incidentes de seguridad de la información que se le reportan. • Mantiene contacto con los miembros del equipo para coordinar sus actividades.

Coordinación de Soporte, Seguridad de la Información y Administración de Redes	• Analizar los incidentes de seguridad que ocurren, así como, acordar e implementar las acciones para eliminarlos y evitar que suceda nuevamente un incidente similar. • Tecnología apoya en cuestiones técnicas, por ejemplo, obtención de *logs*, identificando recursos informáticos involucrados en el incidente, detectando vulnerabilidades en equipos de cómputo o comunicaciones (parches no aplicados, configuraciones inseguras, etc.) • El Administrador de Soporte y Seguridad de la Información participa documentando y reportando el incidente, realizando un dictamen de la situación, coordinando las actividades que den solución al incidente. • Los representantes del área usuaria participan en la determinación del impacto del incidente sobre el negocio. • Otros integrantes del equipo de la Coordinación de Soporte y Seguridad de la Información como por ej. Recursos Humanos, actúan de acuerdo a su especialidad manteniendo en todo momento informado al Responsable de la coordinación.

DESARROLLO DEL PROCEDIMIENTO

Detección de Incidentes de Seguridad.

No.	Descripción
1.	Cualquier empleado o cliente puede identificar un posible incidente de seguridad de la información o percatarse de que uno ya ocurrió de acuerdo a como se realiza el trabajo. Todos los empleados y externos que manejan información y/o recursos informáticos de la Empresa deben estar atentos para detectar y reportar todos los incidentes, posibles y reales, oportuna y apropiadamente.
2.	Cuando un empleado cree estar frente a un incidente de seguridad, debe analizar el mismo conforme a la definición de un incidente, a los ejemplos dados en la introducción y apoyándose en las preguntas del punto 3 de la sección Reporte de Incidentes de Seguridad para que, en caso de tratarse de uno, lo reporte conforme a lo siguiente.

Reporte de Incidentes de Seguridad.

No.	Descripción
1.	Una vez detectado un incidente, la persona que lo detecte debe informar, **inmediatamente** a su Jefe inmediato y/o al responsable del Coordinación de Soporte y Seguridad de la Información.
2.	Si se requiere confidencialidad o por alguna razón se sospecha que algún supervisor o miembro de la Gerencia está involucrado en un incidente, **no debe confrontarlos**, sino reportar el incidente a Dirección.

3.	Para incidentes reportados a la Dirección, el responsable de la Coordinación de Soporte y Seguridad de la Información realiza un análisis con el fin de determinar si el reporte debe ser considerado como un incidente de seguridad. Las siguientes preguntas son una ayuda para realizar el análisis, considerando que, si al menos una respuesta es afirmativa el evento debe catalogarse como incidente de seguridad: ¿Está en riesgo la integridad, disponibilidad o confidencialidad de información sensitiva? ¿Se ha comprometido la confidencialidad de una o varias cuentas (User ID, password)? ¿Hay o puede haber destrucción de datos? ¿Está en riesgo o se perdió la integridad del sistema, existe degradación o negación del servicio? ¿Se ha hecho uso no autorizado de recursos corporativos? ¿La imagen de la empresa está siendo o puede llegar a ser afectada? ¿Se ha divulgado información confidencial que tenga afectación sobre los clientes, en las relaciones de negocio con otras instituciones, de tipo legal o sobre proyectos estratégicos?
4.	Si se define que efectivamente se trata de un incidente de seguridad el Responsable de la Coordinación de Soporte y Seguridad de la Información realiza una evaluación inicial del nivel de Severidad / Impacto, conforme a la tabla del Cuadro 1, documenta el incidente en el formato correspondiente y lo notifica de inmediato a Gerencia. El Responsable de la Coordinación de Soporte y Seguridad de la Información será el único facultado para reportar los incidentes potenciales o reales a la Gerencia tan pronto sean detectados. Si el incidente se trata de la pérdida de equipo de cómputo se debe llenar adicionalmente el Reporte de pérdida de equipo de cómputo. Las notificaciones de incidentes se podrán hacer al Responsable de la Coordinación de Soporte y Seguridad de la Información vía correo electrónico y telefónicamente, toda notificación debe ser acompañada de la siguiente documentación: ✓ Formato de Reporte de Incidente. ✓ Toda la información relacionada al incidente que se considere importante. En caso de que el Responsable de la Coordinación de Soporte y Seguridad de la Información determine que el reporte no corresponde a un incidente de seguridad, debe enviar un correo con la siguiente información: ✓ Descripción y análisis de evaluación del evento, especificando la razón por la que el reporte no es considerado incidente de seguridad. Este correo debe ser enviado a Gerencia en un lapso no mayor a 7 días hábiles a partir de la ocurrencia del evento.

Atención de Incidentes de Seguridad.

No.	Descripción
1.	Cuando el Responsable de la Coordinación de Soporte, Administración de Redes y Seguridad de la Información recibe un Reporte de Incidente de Seguridad, lo analiza para verificar que realmente se trate de uno y revalúa su severidad. En caso de tratarse de un Incidente de Seguridad, convoca, vía mail o telefónica, a los demás miembros correspondientes a la Coordinación de Soporte, Administración de Redes y Seguridad de la Información. En caso de no tratarse de un Incidente de Seguridad lo rechaza informando a quien se lo entregó el motivo por el que no debe considerarse como un Incidente.
2.	Durante la reunión, los miembros de la Coordinación de Soporte, Administración de Redes y Seguridad de la Información evalúan el incidente y obtienen el Nivel de Severidad / Impacto y definen el grado de escalamiento que corresponda, en base a los siguientes criterios: ✓ De acuerdo a la evaluación de Severidad / Impacto, el Responsable de la Coordinación de Soporte y Seguridad de la Información debe notificar a la Gerencia según lo establecido en el Cuadro 1. ✓ El Responsable de la Coordinación de Soporte y Seguridad de la Información determina en base a las evidencias y riesgos del incidente su escalamiento a la Gerencia. Se debe prevenir el escalar prematuramente. ✓ Generalmente los incidentes de nivel de Riesgo/Impacto Medio se escalan solo a nivel Gerencia, mientras que los de Riesgo/Impacto Alto, Emergencia, Críticos se escalan a nivel de Dirección. ✓ Todos los incidentes de conductas sospechosas de empleados o externos (proveedores, consultores, etc.) deben ser reportados a la Coordinación de Soporte y Seguridad de la Información. ✓ Los incidentes relacionados con cuestiones legales deben ser reportados al área de Jurídico. ✓ Los incidentes relacionados con cuestiones laborales deben ser reportados al área de Recursos Humanos. ✓ Los incidentes que afecten la imagen del la empresa deben ser reportados al área de Gerencia.
3.	Para todos los incidentes, la Coordinación de Soporte, Administración de Redes y Seguridad de la Información define las acciones inmediatas que deben llevarse a cabo para contener, a la brevedad, el incidente. El Responsable de la Coordinación de Soporte y Seguridad de la Información coordina que se registren las mismas en el Reporte de Incidente de Seguridad y que se den las instrucciones necesarias.

4.	Por otro lado, el equipo define un **Plan de Acción Correctivo** para corregir o eliminar el incidente, el cual contempla la asignación de actividades y responsables. El Responsable de la Coordinación de Soporte y Seguridad de la Información coordina que se registre en el Reporte de Incidente de Seguridad la información correspondiente. Durante el análisis de cada Incidente, el Administrador podría detectar las causa raíz de algunos de los incidentes o tener propuestas acerca de acciones correctivas definitivas para que éstos no se vuelvan a repetir. En este caso, el Responsable de la Coordinación de Soporte, Administración de Redes y Seguridad de la Información pide al Coordinador del negocio afectado que coordine la entrega de dichas propuestas a los involucrados para que estos decidan si se toman o no las acciones necesarias.
5.	El Responsable de la Coordinación de Soporte y Seguridad de la Información debe vigilar que se den las siguientes condiciones para el manejo de incidentes: ✓ Si el incidente no requiere nivel de escalamiento el Responsable de la Coordinación de Soporte y Seguridad de la Información atenderá el Incidente, o bien, designará a otro integrante de de la Coordinación. ✓ La resolución de un Incidente tiene una prioridad alta. ✓ La información concerniente a un incidente será proporcionada únicamente a las personas que de acuerdo a sus funciones la requieran. ✓ Durante un incidente nada deberá ser creado o destruido, a menos que sea explícitamente aprobado por el Responsable de la Coordinación de Soporte y Seguridad de la Información ✓ La Coordinación de Soporte y Seguridad de la Información deberá realizar un reporte de toda la información registrada sobre un incidente; esta revisión estará dirigida a verificar la calidad, contenido y congruencia de la misma.
6.	La Coordinación de Soporte y Seguridad de la Información del negocio en que se detectó el incidente, elabora las minutas de todas las reuniones o llamadas realizadas hasta que el incidente queda cerrado.
7.	En el caso que se detecte un incidente de seguridad en que se afecte los procesos del cliente, debe activarse la comunicación para el contacto con los niveles autorizados de cada cliente para este fin, para esto se implementará un árbol de llamadas donde en cada nivel se especificarán los datos de los personas, cargo, correo, teléfonos y los niveles de resolución permitiendo establecer así los distintos niveles de escalamiento. **Ver árbol de llamadas de cada cliente.**

Seguimiento y Cierre de Incidentes de Seguridad.

No.	Descripción
1.	El Responsable de la Coordinación de Soporte y Seguridad de la Información coordina y verifica que los responsables de llevar a cabo cada una de las actividades descritas en los diferentes Planes de Acción Correctiva, se lleven a cabo, conforme a lo que se estableció en el Reporte de Incidentes y a lo acordado durante las reuniones de la Coordinación.
2.	Los miembros de la Coordinación de Soporte y Seguridad de la Información responsables de cada actividad de solución, van reportando al Responsable del de la Coordinación el estatus de las mismas y entregándole la evidencia derivada al mismo.
3.	El Responsable de la Coordinación de Soporte y Seguridad de la Información registra en su Reporte de Seguimiento los incidentes, las acciones correctivas planteadas y el estatus en que se encuentra el mismo.
4.	Una vez realizadas y verificadas las acciones correctivas planteadas, la Coordinación de Soporte y Seguridad de la Información analiza si puede declarar como cerrado el incidente. En caso de no quedar cerrado, se plantean las acciones faltantes y se registran en el Reporte de Incidente para que el Responsable coordine que se lleven a cabo.
5.	La Coordinación de Soporte y Seguridad de la Información deberá realizar un análisis de toda la información reportada sobre el incidente; esta revisión estará dirigida a verificar la calidad, contenido y congruencia de la misma.
6.	El Responsable de la Coordinación de Soporte y Seguridad de la Información registra el cierre del incidente en su Reporte de Seguimiento, notifica y le entrega a Gerencia copia del Reporte de Incidente de Seguridad final y del cierre de su Incidencia en el Reporte de Seguimiento.
7.	Si el caso es escalado al cliente a través del árbol de llamadas y se cerró. Se requerirá un documento del cierre del caso por parte del cliente.

Lecciones Aprendidas.

No.	Descripción
1.	Pueden encontrarse valiosas Lecciones Aprendidas y mejores prácticas resultantes de cada incidente. Cuando sea considerado apropiado por la Coordinación de Soporte y Seguridad de la Información y el Responsable de la Coordinación se coordinarán y documentarán un plan de acción a partir de las Lecciones Aprendidas. Este Plan de Acción debe ser implementado tan pronto como el incidente sea cerrado, ya que las lecciones serían olvidadas a menos que sean pronta y adecuadamente documentadas. Esta información no es publicada pero se verifica de forma anual o antes si se presenta algún incidente que se conozca o se tengan referencias anteriores debido a que esta documentación se realiza vía mail y su vigencia es de un año de respaldo dependiendo de su clasificación, por lo cual su tiempo de respaldo máximo es de dos años cuando se trata de incidentes de seguridad de la información.

REGISTROS.

Nombre	Clave (si aplica)	Responsable del resguardo:	Localización:	Medio de almacenamiento, tiempo de retención y disposición de los registros
Reporte de Incidentes de Seguridad	No Aplica	Responsable de la Coordinación de Soporte y Seguridad de la Información	Oficina del Responsable de la Coordinación de Soporte y Seguridad de la Información	Electrónico / 1 año y se elimina
Pérdida de Equipo de Cómputo	No Aplica	Responsable de la Coordinación de Soporte y Seguridad de la Información	Oficina del Responsable de la Coordinación de Soporte y Seguridad de la Información	Electrónico / 1 año y se elimina
Seguimiento a Incidentes de Seguridad	No Aplica	Responsable de la Coordinación de Soporte y Seguridad de la Información	Oficina del Responsable de la Coordinación de Soporte y Seguridad de la Información	Electrónico / 2 años y se elimina

CUADRO 1
Clasificación de Niveles de Severidad e Impacto

Nivel de Severidad / Evaluación de Impacto	**Descripción**	**Tiempo para notificar del incidente**	**Confirma-ción de respuesta por parte de la Coordina-ción**
5 – Bajo*	Incidente donde el impacto es mínimo. Ejemplos de ello son infecciones de virus aisladas, violaciones procesales accidentales, violaciones de procedimientos accidentales, intentos fallidos de violaciones de seguridad a un sistema con criticidad Baja o Media.	2 días hábiles	Al siguiente día hábil de ser notificado.
4- Medio*	Incidente donde exista un impacto moderado al negocio. Ejemplos de esto incluyen intentos fallidos de violaciones de seguridad cualquier sistema, múltiples intentos fallidos de violaciones de seguridad en cualquier sistema crítico, múltiples reportes de correos SPAM maliciosos o virus dentro de un negocio, robo de información Interna de **(su empresa)**, fallas inexplicables de sistemas, interrupción sospechosa (potencial o real) de las actividades propias de un negocio.	Dentro de las primeras 24 horas después de la detección del incidente.	Dentro de las siguientes 24 horas tras la notificación del incidente.
3- Alto	Incidente donde el impacto al negocio puede ser serio. Ejemplos de estos eventos incluyen prácticas maliciosas internas (realizadas por empleados de la empresa), *posibles* violaciones de seguridad a un sistema crítico, violaciones *reales* a sistemas de criticidad Baja o Media, compromiso de información clasificada como Confidencial, sitios de hackers que *pesquen* información de clientes, interrupciones moderadas en las actividades del negocio, salidas de producción de múltiples sistemas y violaciones a leyes locales.	Lo antes posible sin exceder de 4 horas tras detectar el incidente.	Lo antes posible sin exceder de 4 horas tras notificar del incidente.

2- Muy Alto	Incidentes donde el impacto al negocio puede ser severo y representar una crisis para el negocio, o cuando el impacto a la empresa puede ser serio. Ejemplos de esto incluyen interrupciones serias posibles o reales en las actividades del negocio, posible violación de múltiples sistemas de cualquier criticidad, compromiso de información clasificada como Confidencial, violaciones consumadas en sistemas de Alta criticidad.	Lo antes posible sin exceder de 2 horas tras detectar el incidente.	Lo antes posible sin exceder de 2 horas tras notificar del incidente.
1- Crítico	Incidentes donde el impacto a **(su empresa)** pueda ser severo y pueda representar una crisis para la empresa. Ejemplos de esto incluyen la posible interrupción en las actividades, compromiso de información clasificada como Confidencial, impacto público significativo en la reputación de **(su empresa)** o en una postura regulatoria.	Lo antes posible sin exceder de 1 hora tras detectar el incidente.	Lo antes posible sin exceder de 1 hora tras notificar del incidente.

Se verifica la incidencia en el caso que llegue a suceder, según el tipo de incidencia de seguridad, ya sea externa o interna en cuanto a sistemas informáticos, en aquellos procesos donde la data ya fue impresa y esta es manipulada manualmente.

Caso Externo:

a) Se verifican los logs del Firewall Externo e Interno, las entradas y salidas de las PC's, con el fin de descartar que una PC se encuentre bajo el control remoto de algún programa.

b) Si la PC se encuentra operada bajo control remoto externo, se desconecta inmediatamente, para luego estudiar lo sucedido y evitar que ocurra de nuevo.

c) Se evalúa la gravedad de la incidencia por medio de la data o la información sustraída de la PC que fue afectada.

d) Se evalúa si hay complicidad por parte del trabajador que opera la PC. De ser así este será penalizado perdiendo la relación laboral empresa-trabajador de forma justificada.

Caso Interno:

a) Todos los usuarios tienen un único identificador, para utilizar cualquier sistema de la empresa, donde este ID es auditado por Políticas de Seguridad establecidas en el servidor y en cada PC.

b) No pueden utilizar ningún tipo de medio de almacenamiento externo, en el caso de que se descubra al personal será amonestado.

c) Todas las PC's estarán protegidas por el Firewall Interno y Externo

d) Hay bloqueo a ciertas PC's que no pueden tener Internet, debido a que manejan data confidencial.

5.2 Procesos de Administración de Usuarios.

Este proceso se lleva a cabo por el Administrador de Redes.

a) La administración se encuentra centralizada en un servidor principal.

b) Los usuarios están identificados mediante la inicial del primer nombre seguido del apellido, por lo tanto se evita la duplicidad.

c) Las cuentas de los usuarios están organizados y tienen su respectivo acceso según el Departamento a las cuales pertenecen.

d) Solo hay una persona que puede eliminar y agregar usuarios en el servidor, que es el Administrador de Redes.

e) Los password son cambiados cada 20 días obligatoriamente por el servidor, ya que si el usuario no la cambia cuando sea solicitado la cuenta quedara bloqueada.

f) Los derechos de acceso deberán ser solicitados vía correo al Administrador de Redes con copia al Administrador de Seguridad de datos y autorizado por el coordinador o gerente del departamento, el tiempo para otorgar el acceso es de 6 horas después de hacer las verificaciones de seguridad. (ver anexo III)

g) Ningún usuario tiene derecho administrativo en ningunas de las PC's para evitar la instalación de cualquier aplicación, ya sea de código abierto o de terceros.

5.3 Procesos de Revisión de Logs de Seguridad de Usuario.

Para controlar el acceso y actividades los ID de usuarios que se utilizan para todos los procesos del clientes se implementara el siguiente proceso:

a) El administrador de redes de acuerdo a los requerimientos del área de negocios y operativa asignara las claves al personal que procesa los datos de los clientes debidamente autorizados por el administrador de seguridad de información.

b) El administrador de seguridad implantará un procedimiento semanal los días jueves donde revisara las notificaciones realizadas por la revisión del log del gerente de soporte, en donde se evidencie cualquier incidente que afecte el proceso de seguridad y eventos, tales como: Inicio y cierre de sesión, modificación y eliminación en diferentes directorios. La revisión incluirá los logs de las aplicaciones de producción, deberá ser documentado y notificado por mail a la gerencia que reporta y si la incidencia es mayor, la gerencia notificara vía mail a la directiva de los eventos más significativos.

c) La revisión consistirá en verificar la información y si los cambios que se hayan realizado por ingresos, egresos, expiración de claves se hayan aplicado y registrada en los Logs, para identificar si hay algún incidente de seguridad, estos contendrán la siguiente información de manera que permita identificar: Quién, Qué, Cuándo, Dónde y por qué. Así mismo se validará la información registrada en la bitácora de actividades, para comparar cualquier situación fuera de lo normal. En el caso de que se compruebe alguna incidencia debe documentarse y tomar las acciones pertinentes en cada caso.

d) Semestralmente los gerentes de negocio verificarán los derechos de acceso de usuarios para los sistemas y aplicaciones activos, cada gerente documentará la actividad de revisión especificando los usuarios, los accesos y cualquier condición que se requiera.

e) En caso de encontrar alguna incidencia el Administrador de Seguridad notificara al Gerente de Negocio, al Gerente de Talento Humano y al Administrador de Redes la desactivación de la clave de acceso hasta cerrar el caso. Se documentara la incidencia con responsables descripción, causas y acciones en el formulario de riesgo informacional.

5.4 Procesos de Instalación y Actualización del Antivirus, Service Packs y Updates.

a) Solo se permitirá la utilización de Software original legalmente adquiridos y autorizados e instalados por el departamento de sistemas.

b) Los Servidores y las PC's son preparados de la siguiente manera.
   - Se procede a instalar el Sistema Operativo ya sea servidor o cliente
   - Se procede a instalar el Antivirus y configurar los Drivers de los periféricos internos.
   - Se procede a instalar los Service Packs y Updates así como la actualización del Antivirus.
   - Se agrega el Servidor o PC al Dominio, y se procede a eliminar las configuraciones predeterminadas del Sistema Operativo.

c) Aunque los usuarios no tienen derechos administrativos, se prohíbe instalar en las computadoras cualquier tipo de software, ya sean crackeados o no, código abierto, juegos etc.

d) Las actualizaciones serán instaladas por el Dpto. de Soporte Técnico y Seguridad de datos, después de las verificaciones pertinentes y así desplegar el proceso de instalación en cada PC o Servidor, eso se realizara en forma trimestral y los resultados serán notificados por mail a la gerencia

e) Estar atentos de los mensajes de alerta emitidos por el computador. El departamento de sistemas aplicara el detector de virus periódicamente.

5.5 Procesos de Asignación de Tarjetas de Acceso.

El proceso de asignación de las tarjetas es el siguiente:

Ingreso de personal.

a) El gerente de administración le notifica al Administrador de Seguridad de Información el ingreso de un nuevo personal a la empresa.

b) El gerente posee las tarjetas y las claves en una bóveda, esta a su vez se la entrega al responsable de seguridad de información.

c) El Dpto. de Administración debe indicar a que áreas va a tener acceso y en que horario, de manera que la tarjeta sea programada según lo indicado y le sea entregado al nuevo personal.

Egreso de personal.

a) El gerente de administración le notifica al responsable de Seguridad de Información que un empleado culminara labores en la empresa.

b) Se procede a desactivar la tarjeta de acceso.

5.6 Proceso de control de Dispositivos Periféricos

a) Se establece que el uso de dispositivos periféricos tales como: Pen-Drive, Ipod, Lectores de Memoria, Reproductores de Música diferentes a los Ipod, o todo aquel aparato electrónico que sirva como unidad de almacenamiento extraíble está totalmente prohibido, estos son deshabilitados de la siguiente manera.

- Los Puertos USB son deshabilitados por el BIOS y este a su vez posee clave que evita la activación de los mismos.
- Las Quemadoras han sido desconectadas físicamente, tanto el cable de datos como el de alimentación.

6. Proceso de Actualización del Inventario de Hardware y Software

El proceso de actualización del Hardware y Software será de la siguiente manera:

Hardware

- El inventario de Hardware será actualizado cada 6 Meses, cuando adquiera un nuevo PC, Servidor o cualquiera de sus componentes.
- El control del inventario de Hardware se llevara a cabo mediante un archivo de Excel, el cual solo podrá ser accedido y modificado por el personal de Soporte Técnico, Seguridad de datos, Gerentes y Directores.

Software

- El inventario de Software será actualizado cada 6 Meses ó cuando adquiera un nuevo programa, o se proceda actualizar de versiones.
- El control del inventario de Software se llevara a cabo mediante un archivo de Word, el cual solo podrá ser accedido y modificado por el personal de Soporte Técnico, Seguridad de datos, Gerentes y Directores.

7. Proceso de verificación de auditoría de Seguridad (Local, Perímetro externo).

Dentro de las verificaciones de seguridad se establece un procedimiento de verificación del local que incluye la revisión del personal de seguridad física que custodian las instalaciones, sus instrumentos de seguridad y las políticas de uso de las mismas. Así mismo se incluye en el proceso la revisión del perímetro externo que verifica la seguridad de las instalaciones físicas, accesos posibles y los servicios que permiten garantizar la seguridad.

La protección de activos y los sistemas de seguridad físicos son incluidos en la revisión ya que conforman una parte muy crítica para la detección de incidencias, responsables de y aplicar los correctivos correspondientes. Se revisan adicionalmente los procedimientos de seguridad establecidos y su aplicación para evitar el acceso de intrusos. La seguridad de información es también contemplada en la revisión para garantizar las políticas establecidas en este manual.

Esta inspección será realizada trimestralmente por el administrador de seguridad física de la organización que reporta directamente al área administrativa.

Las incidencias o no cumplimientos serán documentados dentro del formulario y notificados a las áreas involucradas (administración, infraestructura, seguridad, sistemas) con descripción, y tiempos de resolución de situaciones o correcciones, responsables y se actualizara con la fecha de cierre una vez que se hayan completado las acciones de corrección de las mismas.

La directiva de ***INCALL*** debe recibir la información de seguimiento ya que posiblemente las soluciones involucren inversiones o gastos que deben ser aprobados y así mismo deberá hacer seguimiento al cierre de las incidencias o no conformidades.

8. Proceso de Autoevaluación de cumplimiento de Políticas.

Con el fin de poder evaluar la aplicación de los estándares y políticas de seguridad de datos, el administrador de seguridad de datos generara trimestralmente un informe de autoevaluación de cumplimiento de políticas en el cual se especificaran los resultados, incidencias y oportunidades de mejora que permitan revisar los procesos, reducir los riesgos y mitigar situaciones críticas.
El resultado de la autoevaluación debe ser enviada a la Directiva de ***INCALL*** y debe ser presentado a los gerentes de negocios involucrados en la operación con el fin de que sean aplicadas las recomendaciones.

9. Políticas de Seguridad Especiales.

Cualquier requerimiento especifico por parte del cliente no contemplado en este manual, será analizado en conjunto e implementado bajo condiciones especiales que serán suplidas con la instalación de PC's, Servidores y enlaces dedicados propios o de INCALL.

Todas las políticas y estándares en este manual han sido diseñados de acuerdo a las políticas de operatividad de la empresa tomando en cuenta la diversidad del servicio a múltiples clientes y plataformas.

9.1 Organización y segmentación de Base de Datos

ESTRUCTURA FISICA

- **EQUIPOS SERVIDORES**
  Disponemos de servidores con tecnología RAID de matriz redundante para proteger los fallos en una unidad de disco única. Además de una copia protegida en servidores de la nube, contra las posibilidades de daños físicos fortuitos: incendios, substracciones,...

- **SISTEMA DE MANTENIMIENTO ELECTRICO Sistema de Alimentación Ininterrumpida (UPS):**
  Contamos con una unidad UPS que nos protege de eventuales problemas de sobrecarga eléctrica, picos de subida y bajada en la alimentación eléctrica de la empresa suministradora de fluido eléctrico. También mantiene mediante acumuladores hasta una hora de energía y avisa en este caso para poder realizar las copias de seguridad y el apagado de los servidores para que no cause efectos un apagado no deseado.

- **EQUIPOS PARA SEGMENTACIÓN DE BASES:**
  Disponemos de 6 equipos que realizan la segmentación de las bases de datos cotejando por diferentes fuentes la validez de los registros según las necesidades del cliente.

- **SERVIDORES EN LA NUBE:**
  Disponemos de 7 copias de seguridad backup uno por cada día de la semana anterior que se van reescribiendo cíclicamente semana por semana en servidores en la nube. De este modo podemos volver a un punto concreto de la semana anterior caso de errores de proceso o de selección de carácter humano.

ESTRUCTURA DE BASES DE DATOS

- **EXCEL:**
  Tenemos diariamente cotejo con motores de búsqueda de prospectos para la segmentación a través de los equipos especializados y motores de búsqueda que se encuentran en la nube. El trabajo con estos motores y la normalización de la data que se envía y recibe bidireccionalmente se realiza mediante el manejo de tablas de Excel.
  Realizamos las modificaciones bien sea por grupos de registros o por registros únicos y vamos transformando una base no amistosa en la base general a la que podemos de esta forma añadir los registros.

- **SQL:**

  Los núcleos de los registros se importan en bases de datos SQL en nuestro caso los registros pasan un último filtro dependiendo de la tipología de clientes basándose en la campaña. En caso de ser campaña de productos similares en universo, tipo de producto y segmento de mercado se agrupan en diferentes bases de datos.

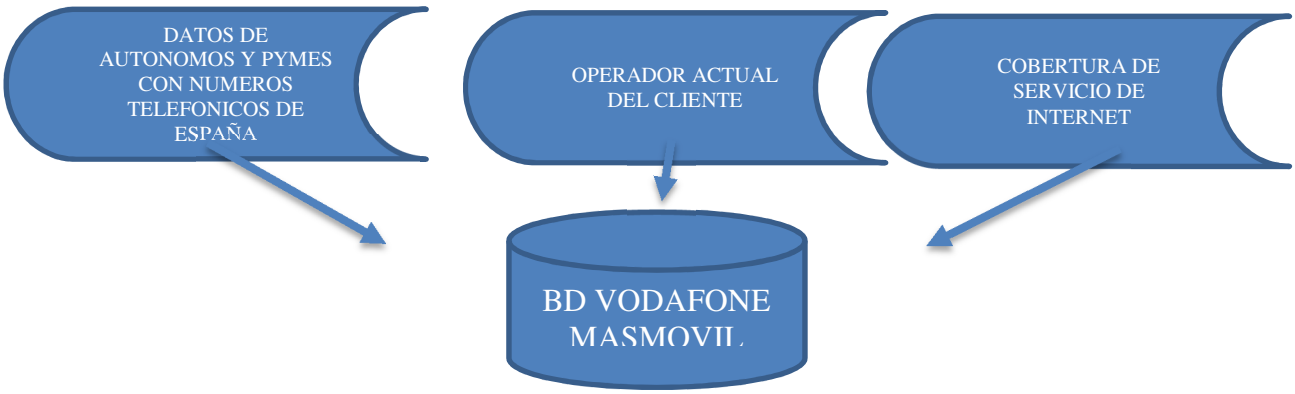
9.2 Segmentación Bases de Datos Mercado Español

BASES DE DATOS DE TELECOMUNICACIONES MERCADO ESPAÑOL

Actualmente tenemos 2 campañas dirigidas al público español del sector de telecomunicaciones como son MASMOVIL y VODAFONE, ambos del mismo segmento, que es profesionales autónomos y pymes.

En este caso utilizamos la misma base de datos donde buena parte de los registros son idénticos y únicamente cambia la capacidad de cada empresa de llevar cobertura del servicio para cada cliente.

De esta manera son 2 bases de datos principales que se alimentan dos a dos como se indica en figura 1. Para cada base hay un motor que recopila los datos necesarios para poder realizar los llamados. En el caso de los llamados a clientes potenciales cumplimos con el requisito de cumplir con el marco legal de clientes que no pueden ser llamados por encontrarse en lista negra como es la **lista Robinson.**



SEGMENTACION BASES DE DATOS MERCADO ESPAÑOL

Disponemos de diferentes métodos de extracción de bases de datos y motores de búsqueda que hacen el trabajo de minería. Principalmente son: Paginas Amarilla de España, QDQ, y Directorio entre otras.

GENERACION BASE DE CLIENTES Y NORMALIZACIÓN

De esos motores extraemos la data principal que incluye, NOMBRE Y APELLIDOS, DIRECCIÓN y NUMERO DE TELEFONO. En el caso de los directorios relacionados con empresas los registros son en su mayoría de empresas y autónomos.
Dependiendo de cada motor utilizaremos diferentes criterios de búsqueda como pueden ser:

DESCARGAR <POR CODIGO POSTAL>
DESCARGAR <POR CALLES>
DESCARGAR <NOMBRES o APELLIDOS>
DESCARGAR <CIUDADES o PROVINCIAS>

Los resultados de las búsquedas nos entregan los datos habitualmente con estas estructuras:

NOMBRE	DIRECCION	CODIGO POSTAL	TELEFONO	TIPO

NOMBRE	DIRECCION	NUMERO Y LETRA	CODIGO POSTAL	TELEFONO	TIPO

NORMALIZACIÓN

Los datos extraídos se encuentran en formato csv (formato de texto separado por comas) o xsl (Microsoft Excel). Sobre estos datos debemos normalizar que los campos utilicen el mismo formato UTF-8 y que no incluyan caracteres especiales excepto las letras que se utilizan en España como pueden ser la Ñ o caracteres como ç (cedilla) del catalán. También normalizaremos todas las palabras que puedan salir con tilde para dejarlas sin ella, á, é, í, ó, ú para ser a, e, i, o, u.
Eliminar cualquier carácter especial diferente y en definitiva normalizar toda la base.

Una vez normalizadas las bases en Excel pasamos el motor de Telecomunicaciones de España que nos entrega el operador con el que se encuentra actualmente y nos completa el registro de este modo:

NOMBRE	DIRECCION	CODIGO POSTAL	TELEFONO	TIPO	OPERADOR

Una vez que tengamos el resultado con operador pasamos a los siguientes motores que nos entrega la cobertura para dar el servicio de internet al cliente ya sea ADSL o Fibra óptica para los dos clientes. VODAFONE y MASMOVIL se van comprobando uno por uno los teléfonos de los clientes. El resultado es añadido a la base anterior que quedaría así:

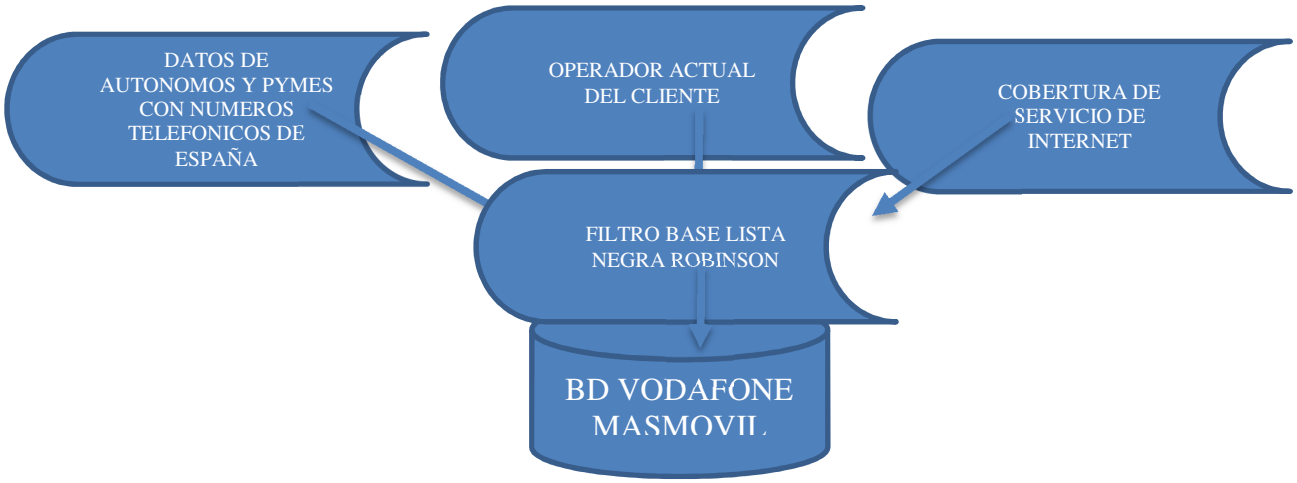
NOMBRE	DIRECCION	CODIGO POSTAL	TELEFONO	TIPO	OPERADOR	VELOCIDAD	VODAFONE (FIBRA/ ADSL)	MASMOVIL (FIBRA/ ADSL)

9.3 Carga de la base de datos a Sistema

En cada paso comprobamos que los datos finales están normalizados y no contienen ningún error. Una vez finalizado el proceso los datos finalmente pasan a una base de datos SQL, desde la cual se llevará el control y actualización periódica incluyendo un campo más que sería fecha última actualización.

9.4 Control de lista Negra

Antes de cargar la base en los sistemas de marcación se pasará un último filtro que según la legislación española debemos eliminar de marcación los clientes que no deseen recibir llamadas comerciales y se encuentran en una base a la que tenemos acceso y bloquea las llamadas, **LISTA ROBINSON**.



10. Formularios de Políticas de Seguridad de la Información

10.1 Login y Password

POLITICAS DE SEGURIDAD DE LA INFORMACION LOGIN Y PASSWORD EN INCALLC.A.

Por medio del presente se le informa al nuevo empleado las normas de seguridad de los datos que se le otorgarán para que pueda acceder al dominio solucioneslaser.com, y así poder utilizar los sistemas necesarios de acuerdos a las funciones del trabajo que va a desempeñar.

Yo XXXXXXXX Administrador de Seguridad de la Información, le hace entrega formal mediante este documento un login y un Password, al Ciudadano: _____

Portador de la Cédula de Identidad: _____

- El login entregado es permanente, el Password lo podrá cambiar al momento de iniciar por primera vez en sistema.

  Características que rigen sobre el Login y el Password
  - Login: esta formado por la iniciar del Nombre seguido del Apellido. En el caso que halla dos empleado con el mismo Nombre y Apellido, se utilizara la inicial del segundo Nombre o Segundo Apellido.
  - Password: Tiene como mínimo 8 caracteres alfanuméricos y especiales: ejemplo: @ _ * #, hasta un máximo de 14 caracteres.
  - El Password tendrá cifrado reversible.
  - El Password tendrá almacenado un historial de hasta 5 Password anteriores, esto es para evitar de que se utilicen datos fáciles que

pertenecen a cada usuario tales como fecha de nacimiento, aniversario, cumpleaños, año de graduación, etc.

- El Servidor de Dominio pedirá un cambio de Password cada 20 días.
- El Login y el Password se bloqueará, cuando se halla intentado iniciar sesión 3 veces, y estas hallan fallados.
- Se procederá de la siguiente manera:
    - El Usuario se comunicará con el Administrador de seguridad de la Información y le explicará lo sucedido.
    - El Administrador imprimirá un Mail con 3 copias indicando el nombre y cargo del empleado y el desbloqueo de la cuenta después de haber estudiado el hecho.
    - La primera copia del Mail será para el empleado, la segunda copia será para el departamento de Recursos Humanos para que sea anexada al expediente del trabajador y la tercera para el Administrador de Seguridad de la Información.

- Está prohibido que el Login y el Password otorgado al usuario sea divulgado tanto fuera como dentro de la empresa. Es intransferible.

- Se le recomienda al usuario no escribir ni el Login ni el Password en ningún papel para evitar que los datos sean visualizados.

- Se le recuerda que el uso indebido del Login y el Password, será penalizado según la gravedad del hecho ocurrido.

10.2 Desactivación del Login y el Password

DESACTIVACION TEMPORAL:

- **Vacaciones:** Se desactiva después de la notificación de recursos humanos vía mail, de acuerdo al tiempo que durará las vacaciones,

- **Reposo:** Se desactiva después de la notificación de recursos humanos vía mail, de acuerdo al tiempo que durará el reposo,

- **Permiso Remunerado o no Remunerado:** Se desactiva después de la notificación de recursos humanos vía mail, de acuerdo al tiempo que durará el permiso.

DESACTIVACION DEFINITIVA:

- **Despido:** Se precederá a eliminar, después de la notificación de recursos humanos vía mail.
- **Renuncia:** Se precederá a eliminar, después de la notificación de recursos humanos vía mail.
- **Muerte:** Se precederá a eliminar, después de la notificación de recursos humanos vía mail.

Nota: El empleado acepta las condiciones de este documento.

XXXXXXXXXXXX **Nombre y C.I:**

Administrador de Seguridad **Cargo:**

10.3 Desbloqueo y Reseteo del Login y el Password.

POLITICAS DE SEGURIDAD DE LA INFORMACIÓN
ACTUALIZACION O DESBLOQUEO
DEL LOGIN Y EL PASSWORD EN INCALL

Por medio de la presente se le notifica al Empleado(a)_____, que debido al mal uso de su Login y password se le entrega el siguiente Memo como advertencia ya que luego de 3 será entregada una amonestación. Así mismo se le advierte que debe tener más cuidado en un futuro y de tener algún inconveniente con su Login y password comunicarse con el Administrador de Seguridad de la información inmediatamente, sea cual sea el motivo de la falla (olvido o negligencia). Por otro lado si se verifica que la cuenta esta siendo utilizada por otra persona se realizará una amonestación directa e inmediata, por incumplir las normativas de Seguridad de la Información.

De manera que para su conocimiento se hacen tres copias de este ejemplar, con los siguientes fines.

- 1era Copia: Esta se queda con usted
- 2da Copia: Esta se entregará al departamento de Recursos Humanos para que se anexe a su expediente.
- 3ra Copia: Esta se quedará en el Dpto. de Seguridad de la Información para ser anexa en un expediente del personal para control.

Se le recuerda que el Login y el password son datos delicados e intransferibles, por lo que es necesario no divulgar su password aunque este sea solicitado por su jefe inmediato.

En el caso que de que se verifique que otro usuario este utilizando otra cuenta que no le halla sido asignada, se amonestaran severamente, a los dos empleados, tanto al que pertenece la cuenta como al que le esta dando uso.

XXXXXXX **Nombre y C.I:**

_____ _____

Administrador de Seguridad **Cargo:**

10.4 Riesgo Informacional.

Riesgo Informacional

Area: _____ ***Fecha:*** _____

Proceso:

Causa de Incumplimiento:

Justificación:

Riesgos relacionados:

1.
2.
3.

Responsable del Proceso: ***Turno:***

	Nombre	***Firma***	***Fecha***
Solicitado Por:			
Elaborado Por:			
Aprobado Por:			

Observaciones:

10.5 Listado de Verificación de Auditoría de Seguridad.

Lista de Verificación de Auditoría de Seguridad

Verificar Respuestas y llenar – Si la respuesta a cualquiera de las partes fuera no , se debe indicar "NO" en el espacio de respuesta.

Nota: N/A significa no aplicable

Información General			
Nombre de la Sede /División/Gerencia:		Fecha:	
Dirección Edificio:			
Cantidad de pisos de todo el edificio:		Cantidad de pisos ocupados por INCALL.	
Cantidad de guardias:		Cantidad de Empleados:	
Nombre de Funcionario/Responsable de Seguridad:			
Gerente:			
Persona que ejecuta la inspección:			

Inspección General del Local

Sección 1 Administración de Seguridad

	Si	N	N/		Si	N	N/
a) Se mantiene el Archivo de seguridad / *Security File* de acuerdo a la política de Seguridad de INCALL?				b) Tiene Instrucciones de Puesto por escrito para los guardias?			
c) Si tiene guardias armados, se ha presentado una política de excepción y ha sido aprobada por el departamento de Seguridad o tiene una copia de las leyes locales que requieren guardias armados?				d) Si se almacenan armas en locales de INCALL se guardan y controlan de conformidad con la Política de Seguridad de INCALL?			
e) Los guardias usan uniformes identificables?				f) Sabe quién es y cómo contactar a su Administrador de Seguridad?			
g) La empresa de seguridad provee un gerente de cuenta o persona de contacto para el negocio?				h) El Administrador de Seguridad del Local designado ha sido capacitado?			

i) La empresa de guardia responde a sus necesidades y preocupaciones?					j) Las políticas de excepción son presentadas para su re-aprobación por DEPARTAMENTO DE SEGURIDAD anualmente?				
k) Se ha presentado una política de excepción a departamento de Seguridad para todas las variaciones a la Política de Seguridad de INCALL?					l) Los empleados y guardias han sido capacitados en:				
m) Se presentan los Reportes de Incidentes al Administrador como lo requiere la Política de Seguridad?					➢ Procedimientos de Informes de Incidentes				
					➢ Procedimientos de Violencia en el Lugar de Trabajo				
					➢ Procedimientos de Amenaza de Bomba				
					➢ Evacuación de Emergencia				

Sección 2 Perímetro Externo

	Si	N	N/			Si	N	N/
a) Un mínimo de dos empleados (*staff*), al menos un funcionario, abre la Sede, con guardias de seguridad cuando es necesario.					b) Si así fuera, la reja o pared están en buen estado?			
c) Todas las puertas de entrada funcionan y Están en buen estado?					d) Las puertas y ventanas externas del edificio están en buen estado?			
e) Se presentan áreas externas alrededor del edificio sin iluminar ?					f) Los lugares de carga y descarga y otros puntos de entrada están asegurados?			
g) Las cerraduras de ventanas y puertas funcionan apropiadamente?					h) Existen áreas externas alrededor del edificio sin iluminar?			
i) Todas las luces externas funcionan?								

Sección 3 Protección de Activos

	Si	No	N/			Si	No	N/

a) Se han implementado los procedimientos de apertura y cierre según la clasificación del local conforme a la Política de Seguridad de INCALL					b) Se emplea el control dual en la apertura de cajas de seguridad conforme a la Política de Seguridad de INCALL?				
c) Se controlan los sistemas de alarma mensualmente?									

Sección 4 Procedimientos de Seguridad

	Si	No	N/			Si	No	N/
a) Se aplican los procedimientos para evitar que personas no autorizadas tengan acceso al edificio?					b) Son los procedimientos de control de acceso efectivos para la prevención del acceso de personas no autorizadas al edificio?			
c) Se aplican procedimientos de control de acceso adicionales para restringir el acceso solo a empleados autorizados a Centros de Datos y otras áreas de alto riesgo?					d) Tiene planes de evacuación y emergencia por escrito de INCALL. para emergencias tales como amenazas de bomba?			
e) Tiene una lista y el plan de notificación actualizado con los nombres y teléfonos?								

Sección 5 Seguridad de la Información

	Si	N	N/			Si	N	N/
Se aplica un proceso de destrucción de documentación confidencial o restringida o de información de los clientes?					Los empleados se adhieren a la política de “escritorio ordenado” descrita en la política de seguridad de DEPARTAMENTO DE SEGURIDAD?			
Los empleados previenen el acceso no autorizado a información del negocio en el área de trabajo? Incluyendo, grabaciones, documentación, etc.?					Los empleados mantienen los armarios de archivo y oficinas asegurados?			

Sección 6 Sistemas de Seguridad

	Si	N	N/			Si	No	N/ A
Los sistemas de alarma están conectados las 24hrs a una Estación de Monitoreo Central?					Se inspeccionan diariamente las cámaras de Seguridad para asegurar la calidad de la imagen y el correcto funcionamiento de las cámaras?			
Se guarda mensualmente las grabaciones de las cámaras de seguridad y se guardan de conformidad con las políticas en vigencia?					Se chequea diariamente el buen funcionamiento del disco duro donde reside la grabación?			
Se verifica la calidad de grabación y de reproducción de las imágenes grabadas?					Todas las puertas exteriores están equipadas con cerraduras de seguridad?			
Los procedimientos de control de acceso son efectivos en la prevención del acceso no autorizado al área donde se guardan la grabaciones?								

Sección 7 Sección de Resolución y Seguimiento de Auto-Auditoría de Seguridad

Indicar a continuación la resolución de riesgos asociados con una respuesta “NO” en la Auto-Auditoría. Cualquier riesgo que no pueda ser resuelto en 30 días debe ser referido al Administrador de Seguridad quién trabajará con el Negocio para determinar un tiempo razonable de resolución y/o controles compensatorios.

Aclarar número de sección y letra, una breve explicación y el tiempo determinado para corregir cada riesgo identificado. Cuando cualquier riesgo sea corregido se debe notificar al Administrador de Seguridad.

Número / letra de Sección:	Tiempo para Corregir:
Breve descripción:	Riesgo: Alto Medio Bajo
Persona responsable:	Fecha corregido:

Número / letra de Sección:	Tiempo para Corregir:
Breve descripción:	Riesgo: Alto Medio Bajo
Persona responsable:	Fecha corregido:

Número / letra de Sección:	Tiempo para Corregir:
Breve descripción:	Riesgo: Alto Medio Bajo
Persona responsable:	Fecha corregido:

Número / letra de Sección:	Tiempo para Corregir:
Breve descripción:	Riesgo: Alto Medio Bajo
Persona responsable:	Fecha corregido:

Número / letra de Sección:	Tiempo para Corregir:
Breve descripción:	Riesgo: Alto Medio Bajo
Persona responsable:	Fecha corregido:

Número / letra de Sección:	Tiempo para Corregir:

Breve descripción:	Riesgo: Alto Medio Bajo
Persona responsable:	Fecha corregido:

Número / letra de Sección:	Tiempo para Corregir:
Breve descripción:	Riesgo: Alto Medio Bajo
Persona responsable:	Fecha corregido:

Realizado por:

Aprobado por: