PROYECTO DE CERTIFICACION 27001

IMPLEMENTACIÓN DE

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

DE LA EMPRESA ACB INGENIERIA S.A.

Índice General

Índice de Ilustraciones

CAPITULO 3: Etapa 1: Planeación

Índices de Tablas

CAPITULO 4: Análisis de Riesgo

CAPITULO 5: Etapa 2: Hacer

ANEXOS

CAPÍTULO 1
MARCO REFERENCIAL

1. Marco Referencial

ACB INGENIERIA requiere implementar la norma ISO 27001 en respuesta a la la gran cantidad de datos (Big Data) que la empresa ha debido enfrentar, y es en el mejor interes de ACB, de sus clientes y de la nueva escalada mediatica que se presenta en el mercado e industria servicios TI, es por ello que la Norma ISO27001 se posiciona como el ente valuador sobre la gestión de calidad y seguridad lo que permite tener una validez en la seguridad de bases y servicio a nivel nacional con estandar internacional, Permitiendo a la empresa que posea dicha certificación escale sus servicios de seguridad y manejo de datos a un modo confiable, de absoluta vigilancia y crebilidad a sus clientes.
Para ACB INGENIERIA la Norma Iso 27001 surge como la respuesta obvia y más eficiente, que es hoy en dia uno de los activos más valiosos que hoy en día poseen todas las diferentes empresas, que son: La información, La Transparencia, y La Confianza.
Estos tres principios son los que hoy en dia un activo el cual hay que proteger en un mundo tecnológico cada vez más susceptible a sufrir grandes amenazas en cuanto a su confiabilidad y al resguardo de su informacion. De igual forma la información es vital para el éxito y sobrevivencia de las empresas en cualquier mercado. Con todo esto todo parece indicar que uno de los principales objetivos de toda organización es el aseguramiento de dicha información, esté a salvo de depredadores tecnológicos y también de los sistemas que la procesan.
Para este propósito es que ACB Ingenieria considera que una adecuada gestión de la seguridad de la información y certificación de seguridad dentro de las organizacion, permitirá implantar los cambios y mejoramientos necesarios en nuestro sistema, que aborden plenamente la tarea de proteger la informacion de nuestros clientes y potencie un mejoramiento considerable en el personal calificado, proporcionandoles herramientas y procesos eficientes que en forma metódica y lógica, documentada y basada en objetivos claros evaluación de los riesgos y de seguridad de la información, creará el ambiente fluido, transparente y confiable, principios por los que ACB Ingenieria se basa como parte de su visón y misón como empresa de servicios TI en Chile y Peru.
Para lograr estos objetivos, ACB Ingenieria necesita especializarse como ente confiable que trabaja bajo los estándares internacionales de resguardo de datos y seguridad de la información, específicamente trabajar con los estándares que se encuentran en la norma ISO 27001.
Gracias a la Norma ISO 27000 , ACB podrá implementar una serie de estándares que proporcionen y promuevan un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar nuestro Sistema de Gestión de Seguridad de Información.
La decisión estratégica de adoptar este estándar fue hecha en base a al diseño e implementación desde la Jefatura hasta los mandos Junior de la organización, ya que permitirá escalar su implemenatción a todas las áreas y departmanetos de la organización.

La aplicación de este standard también requiere de un vocabulario definido, que evite las interpretaciones de conceptos técnicos y de gestión equivocados con el fin de tener

un marco de gestión de la seguridad de la información en común, utilizable por cualquier todos en la organización.
El objetivo y la decisión de desarrollar un sistema de gestión de seguridad de la información bajo un standard internacional se da como resultado de varias investigaciones realizadas por la empresa IDC en los últimos 5 anos señalan que nuestro mercado objetivo que se compone por la mediana empresa chilena y latina en general, tiene miedo al concepto de servicios de la nube "iCloud", o la desconoce, sea que lo vean como un concepto abstracto que no entienden o porque gran parte de las empresas que segun Sercotec en su ultimo estudio senala que Las Grandes empresas solo el 8.1% esta en iCloud y el 3.1% de la Mediana entiende o confia en los servicios icloud. Por lo que se concluye que la gran mayoria de la mediana y grande empresa en Chile se atemorizan de que sus datos esten en la nube en lo que ellos llaman „a disposición de todo el mundo" y que es mejor tener su informacion y datos en sus precarias salas de servidores, sin ninguna medida de seguridad, control, encriptación, alta disponibilidad o de un mínimo estándar de calidad pero dentro de sus perimetros.

Basandonos en estos puntos es que la ACB quiere facilitar la transición del empresariado a la Nube. Disminuyendo el número de amenazas y acreditando el Cloud de ACB Ingenieria que tome características de un Icloud de nivel mundial , que cuente con todas las certificaciones de seguridad, calidad y privacidad que son requeridas para operar con tanto o más condiciones que un ambiente de servicios de datacenter tradicional. En el cloud ACB Ingenieria la seguridad y privacidad de la información es un tema fundamental y por lo mismo está resuelto a realizar los cambios y adquirir los estandares necesarios para facilitar la confianza de sus clientes en los servicios que ACB ingenieria provee como fortalecer las vulnerabilidades existentes en sus clientes como mantener alejados y protegidos los a activos de información de sus clientes, de diversas formas de fraude, sabotaje o vandalismo, como también las amenazas que pueden considerarse de mayor relevancia en la institución como son los virus informáticos, la violación de la privacidad de los empleados, los empleados deshonestos, intercepción de transmisión de datos o comunicaciones y/o fallas técnicas de manera voluntaria o involuntarias.

Es por ello que a la par de la Certificación bajo el estándar ISO 27001 es relevante la importancia de realizar el análisis referente a la gestión de sus departamentos es pertinente.
Por lo tanto las departamentos que serán implementados son:

1. Jefatura /Adminitración
2. Operaciones :
    i. Internas - Development
    ii. Externas - Datacenter
3. Ventas
    i. Internas -
    ii. Externas - Callcenter
4. Marketing / Relaciones Publicas
5. Departamento de Recursos Humanos

En esta sección veremos el departamento de Recursos Humanos :

En este departamento debemos conocer y reconocer las debilidades y fortalecer las herramientas en los empleados y el manejo de la información correspondiente a esta área y su flujo dentro de la empresa. De esta manera, se establece que los miembros de este team mayor de la empresa posee los debidos conocimientos técnicos y sabe cómo manejar la información y establecer los procedimientos debidos para resguardar dicha información tanto de amenazas internar como externas, implementando procedimientos, controles u observaciones de su funcionamiento dentro del área dispuesta, los cuales permitirán desarrollar cambios en los mismos.

La empresa ACB INGENIERIA requiere implementar un sistema de gestión de seguridad de la información con respecto a los recursos humanos debido bajo estos lineamientos del estándar ISO 27001 se permitirá reclutar personal calificado de acuerdo al rol a desempeñar. La empresa como Garanante de la información y datos vitales de sus clientes, la cual se considera delicada y confidencial, no se puede arriesgar a incorporar personal que pueda hacer mal uso, voluntaria o involuntariamente, de ésta.

ACB INGENIERIA considera que una selección adecuada de su personal bajo los requerimientos de ISO 27001, permitirá crear una base de confianza sólida donde la Mediana y Gran empresa en Chile, sentirá confianza en creer y aplicar los sistema de gestión de seguridad de la información de ACB ingeniería en sus empresas. La empresa desea ser pionera en la implementación de dicho sistema, ya que dentro de su mercado es muy escaso el conocimiento del tema.

CAPÍTULO 2
GENERALIDADES DE LA EMPRESA

2. Generalidades de la Empresa:

2.1 Antecedentes de la empresa:

La Compañía se constituyó con la denominación de ACB INGENIERIA S.A., mediante Escritura Pública autorizada por el Notario _____, el _____de mil novecientos ochenta y cinco, inscrita en el Registro de la Camara de Comercio de Santiago el _____del mismo año, con un capital suscrito y pagado de (PCL$ 0.000.000,00).

ACB INGENIERIA es una sociedad de responsabilidad limitada. Autorizada y controlada por _____. Su casa matriz está ubicada en la ciudad de Santiago en la calle Nueva de Lyon 145, Piso 4th, No. 404, 7510054 Providencia, Santiago, Chile, y su filial está ubicada en Perú: Av.Benavides 620, Of.805, Miraflores, Lima, Perú.

ACB INGENIERIA , opera y brinda sus servicios al amparo de:

- La Ley de Mercado de Telecomunicaciones del Gobierno Chileno y Peruano
- Su Reglamento General,
- El Reglamento para el Funcionamiento de Datacenter, y empresas de Informacion
- En su reglamentación interna y Manuales Operativos.

ACB INGENIERIA no tiene accionistas ni inversores externos, siendo patrimonio familiar 100%.

ACB INGENIERIA cuenta con una certificación ISO 9001:2008 en los siguientes procesos:

-
-

2.2 Descripción del funcionamiento del área Recursos Humanos

2.2.1 Selección de personal

ACB ingeniería recibe los datos del postulante mediante una carpeta enviada por correos o por email conteniendo: Carta de Presentación (motivación), CV, Copias de Certificaciones, y Cartas de referencias. En seguida se separan por datos que los CV contienen , específicamente técnicos, materias, anos de experiencia en los temas y rubros que se requieren, y se analiza los datos del postulante y si le evalua considerando su aptitud para el cargo vacante. Si no es así se recicla y se comprueba si el perfil puede

ser utilizado en alguna de las posiciones vacantes de la empresa. De lo contrario se archiva para posterior contratación, en caso de que se requiera.

Antes de iniciar el reclutamiento de personal, se presenta primeramente un análisis interno de la empresa , promoción de colaboradores que puedan ser promovido o reasignado para ocupar la vacante. En caso de realizar el reclutamiento de personal, se preseleccionan algunos CV y se realizan entrevistas.

2.2.2 Contratación de personal

El proceso de la entrevista se consideran diferentes etapas de Calificación:
Iniciándose con una pre-selección de candidatos, luego la selección de los candidatos se les realizará una entrevista telefónica, el o los que aprueben la entrevista, se les invitará a las oficinas de ACB ingenieria y se les tomará un test Psicométricos y Técnico de temas específicos a los rubros en los cuales se requieren su expertiz, de acuerdo a la información del perfil del cargo[1] que se requiere. Aquellos candidatos que identifiquemos que tienen los conocimientos adecuados durante la entrevista serán invitados a una entrevista personal con el CIO y el Director de ACB Ingenieria o Gerente de su departamento y a conocer las instalaciones de ACB Ingenieria. Después de una entrevista personal exitosa, al candidato recibirá por correo una oferta formal y una nueva invitación para discutir los temas y próximos pasos. Una vez finiquitada la contratación se coordina la presentación de los documentos para archivo en la Carpeta de Personal. Se elabora el contrato de trabajo y se procede a la obtención de la firma de ambas partes.

2.2.3 Iniciación del cargo

Dependiendo del cargo, el gerente de recursos humanos envía previamente la ficha para archivo del Gerente de operaciones a cargo, y un dia citado, se reúniran el gerente de operaciones , recursos humanos y el postulante, iniciándose asi la integración del mismo a las labores. El gerente de departamento integra al empleado informándole los siguientes aspectos: ubicación de su puesto de trabajo, quien es su gerente inmediato, la estructura del departamento, se le entregará además una lista con las obligaciones y responsabilidades en el **Manual de Funciones**, donde se especifica la descripción de cada cargo[2], supervisando su lectura y comprensión y despejando cualquier duda que tenga al respecto, además se le aclarará quienes están a su cargo, y con quien debe reportarse, su team de trabajo y reglamentos como horarios de trabajo, beneficios y organigrama[3], todo esto estará contenido en una carpeta de bienvenida las cuales además de entregar información de la visión, misión, productos y servicios de la empresa como otros intereses como bien social y sustentabilidad o campanas de acción, también se le entregará , además material con los principios, valores, visión y misión de la empresa detalles que ayudaran a un mejor desempeño de sus actividades e integración al equipo.
En cuanto a material se le entregará un Notebook, estación de trabajo y su ID-Card y un carta firmada por el presidente de la compañía dándole la bienvenida a la empresa.

2.2.4 Durante el empleo

A cada empleado es asignado un equipo informático con su respectiva información de acceso al sistema, cuentas, passwords, para el proceso de protocolos de ingreso y autenticación al sistema de la organización.

[1] Revisar Anexo 3: Perfil o Requisitos de los diferentes cargos.
[22] Revisar Anexo 2: Descripción de cada puesto de trabajo.
[3] Revisar Anexo 4: Organigrama.

2.2.5 Cambio o reubicación del empleado

En caso de cambio de cargo o reubicación del empleado , se realiza la postulación en forma interna, si el candidato es re-ubicado se realiza la documentación que detalle o deje constancia de lo sucedido en un Memorandum de cambio de Rol, se notifica, en forma oral y por email al empleado; y el área de recursos humanos realiza en el sistema el cambio de cargo y por ende, de sueldo. El empeado se reporta con el nuevo gerente inmediato y este le entrega su nuevo Manual de Funciones y responsabilidades , lo presenta brevemente al departamento, lo presenta al sistema para comunicar su cambio de rol , ya que éste nuevo rol le concedan amplitud o restricción en cuanto a accesos y permisos dentro del sistema.

2.2.6 Separación del empleado

Mediante una carta escrita por el Gerente de Departamento de Recursos Humanos de la empresa se le comunica al empleado de la finalización de la relación laboral. En este proceso se finiquitación de su contrato laboral y se inactiva la información de acceso correspondiente a dicho empleado. Se le entrega una carta de agradecimiento por sus servicios, y se le adjunta un listado con los elementos que deben ser devueltos a la empresa y en las condiciones que deben ser devueltos, como así toda identificación acumulada, como también listado de las password/Contraseñas a su cargo. (si hubieran, estas serán comprobadas antes que el deje físicamente la empresa), como también deberá entregar tarjetas ID-Card, llaves, y cualquier otro elemento que lo vincule a la empresa. Los trámites de liquidación son llevados a cabo como un procedimiento perteneciente a la empresa por el departamento de recursos humanos en nombre de la la Gerencia de la Empresa.

CAPÍTULO 3
ETAPA 1: PLANEACIÓN

3. Etapa 1: Planeación

3.1 Definición de la Norma ISO 27002

3.1.1 Seguridad Informática:

Protección de la Infraestructura de las tecnologías de la Información dentro de la empresa. Este tipo de seguridad es importante para la compañía, ya que se encarga de precautelar por el perfecto estado y funcionamiento de los equipos informáticos donde fluye la información. La información reside en medios como estos equipos, soportes de almacenamiento y redes de datos, y teniendo en cuenta estos aspectos, se hace vital mantener la seguridad informática a través de lineamientos de protección.

3.1.2 Gestión de Seguridad de la información

La seguridad de la información es la protección de los activos de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales. Estos activos se pueden detallar como: correos electrónicos, páginas web, imágenes, base de datos, telecomunicaciones, contratos, documentos, etc.
La seguridad de estos activos de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos.
La gestión de seguridad de la información apunta a mantener la estabilidad en los siguientes aspectos con respecto a estos activos:
Confiabilidad: Acceso solo de personal autorizados.
Integridad: Exactitud y completitud de la información y procesos.
Disponibilidad: Acceso a la información y procesos por parte del personal autorizado, cuando lo requieran.

3.1.3 International Organization for Standarization (ISO):

La ISO[4] es una federación internacional con sede en Ginebra (Suiza) de los institutos de normalización de 157 países (uno por cada país). Es una organización no gubernamental (sus miembros no son delegados de gobiernos nacionales), puesto que el origen de los institutos de normalización nacionales es diferente en cada país (entidad pública, privada).
Las normas ISO surgen para armonizar la gran cantidad de normas sobre gestión de calidad y seguridad que estaban apareciendo en distintos países y organizaciones del mundo. Los organismos de normalización de cada país producen normas que resultan del consenso entre representantes del estado y de la industria. De la misma manera las normas ISO surgen del consenso entre representantes de los distintos países integrados a la I.S.O.

[4] Revisar Anexo 1: Definiciones y Términos

3.1.4 ISO 27000, aplicada a la seguridad de la información:

Uno de los activos más valiosos que hoy en día posee las diferentes empresas, es la información y parece ser que cada vez más sufre grandes amenazas en cuanto a su confiabilidad y su resguardo, de igual forma la información es vital para el éxito y sobrevivencia de las empresas en cualquier mercado. Con todo esto todo parece indicar que uno de los principales objetivos de toda organización es el aseguramiento de dicha información, así como también de los sistemas que la procesan.
Para que exista una adecuada gestión de la seguridad de la información dentro de las organizaciones, es necesario implantar un sistema que aborde esta tarea de una forma metódica y lógica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización. Para lograr estos objetivos, existen organizaciones o entes especializados en redactar estándares necesarios y especiales para el resguardo y seguridad de la información, los estándares correspondientes se encuentran en la norma ISO 27000.
La ISO 27000 es una serie de estándares desarrollados, por ISO e IEC[5]. Este estándar ha sido preparado para proporcionar y promover un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de Información. La adopción de este estándar diseño e implementación debe ser tomada en cuenta como una decisión estratégica para la organización; se pretende que el SGSI se extienda con el tiempo en relación a las necesidades de la organización. La aplicación de cualquier estándar ISO 27000 necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión, que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

3.1.4.1 Serie ISO 27000

ISO ha reservado la serie de numeración 27000 para las normas relacionadas con sistemas de gestión de seguridad de la información. En el 2005 incluyó en ella la primera de la serie (ISO 27001), las demás son:

- ISO27000 (términos y definiciones),
- ISO27002 (objetivos de control y controles),
- ISO27003 (se centra en aspectos críticos en la implementación SGSI),
- ISO27004 (desarrollo y utilización de métricas y técnicas de medida de la efectividad de un SGSI),
- ISO27005 (directivas guía para la gestión del riesgo de seguridad de la información)
- ISO27006 (proceso de acreditación de entidades de auditorías, certificación y el registro de SGSI).
- ISO/IEC 27007 Guía de Auditoria de un SGSI

3.1.5 ISO 27001

Es un estándar ISO que proporciona un modelo para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Se basa en el ciclo de vida PDCA (Planear-Hacer-Verificar-Actuar) de mejora continua, al igual que otras normas de sistemas de gestión.

[5] Revisar Anexo 1: Definiciones y Términos

Este estándar es certificable, es decir, cualquier organización que tenga implantado un SGSI según este modelo, puede solicitar una auditoría externa por parte de una entidad acreditada y, tras superar con éxito la misma, recibir la certificación en ISO 27001.

El origen de la Norma ISO27001 está en el estándar británico BSI (British StandardsInstitution) BS7799-Parte 2, estándar que fue publicado en 1998 y era certificable desde entonces. Tras la adaptación pertinente, ISO 27001 fue publicada el 15 de Octubre de 2005.
El enfoque del proceso para la gestión de la seguridad de la información presentado en este estándar internacional fomenta que sus usuarios enfaticen la importancia de:

- Entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información.
- Implementar y operar controles para manejar los riesgos de la seguridad de la información.
- Monitorear y revisar el desempeño del SGSI
- Realizar mejoramiento continuo en base a la medición del objetivo

3.1.6 PDCA (Planear-Hacer-Verificar-Actuar) /Plan, Do, Check, Act

El modelo de proceso PDCA, se detalla a continuación a través de cada una de sus fases:

3.1.6.1 PLANIFICACIÓN

Ilustración 3. 1 Fase Planificación

- Definir alcance del SGSI: en función de características del negocio, organización, localización, activos y tecnología, los límites del SGSI. El SGSI no tiene por qué abarcar toda la organización; de hecho, es recomendable empezar por un alcance limitado.
- Definir política de seguridad: que incluya el marco general y los objetivos de seguridad de la información de la organización, tenga en cuenta los requisitos de negocio, legales y contractuales en cuanto a seguridad.

- Definir el enfoque de evaluación de riesgos: definir una metodología de evaluación de riesgos apropiada para el SGSI y las necesidades de la organización, desarrollar criterios de aceptación de riesgos y determinar el nivel de riesgo aceptable.
- Inventario de activos: todos aquellos activos de información que tienen algún valor para la organización y que quedan dentro del alcance del SGSI.
- Identificar amenazas y vulnerabilidades: todas las que afectan a los activos del inventario.
- Identificar los impactos: los que podría suponer una pérdida de la confidencialidad, la integridad o la disponibilidad de cada uno de los activos.
- Análisis y evaluación de los riesgos: evaluar el daño resultante de un fallo de seguridad y la probabilidad de ocurrencia del fallo; estimar el nivel de riesgo resultante y determinar si el riesgo es aceptable o requiere tratamiento.
- Identificar y evaluar opciones para el tratamiento del riesgo: el riesgo puede reducido, eliminado, aceptado o transferido.
- Selección de controles: seleccionar controles para el tratamiento el riesgo en función de la evaluación anterior.
- Aprobación por parte de la Dirección del riesgo residual y autorización de implantar el SGSI: hay que recordar que los riesgos de seguridad de la información son riesgos de negocio y sólo la Dirección puede tomar decisiones sobre su aceptación o tratamiento.
- Confeccionar una Declaración de Aplicabilidad: Es, en definitiva, un resumen de las decisiones tomadas en cuanto al tratamiento del riesgo.

3.1.6.2 IMPLEMENTACIÓN (HACER)

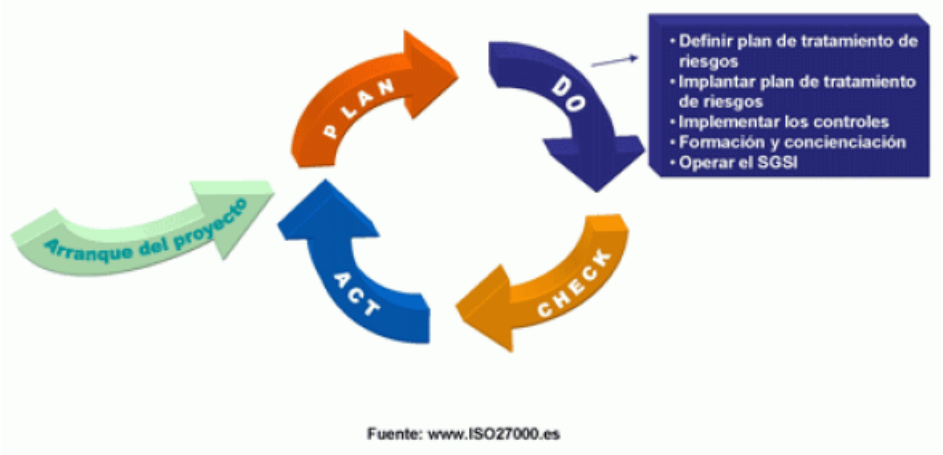


Ilustración 3. 2 Fase Hacer

- Definir plan de tratamiento de riesgos: que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- Implantar plan de tratamiento de riesgos: con la meta de alcanzar los objetivos de control identificados.
- Implementar los controles: todos los que se seleccionaron en la fase anterior.
- Formación y concienciación: de todo el personal en lo relativo a la seguridad de la información.
- Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones.
- Gestionar las operaciones del SGSI y todos los recursos que se le asignen.
- Implantar procedimientos y controles de detección y respuesta a incidentes de seguridad.

3.1.6.3 SEGUIMIENTO (CHEQUEAR)

Ilustración 3. 3 Fase Chequear

- Ejecutar procedimientos y controles de monitorización y revisión: para detectar errores en resultados de procesamiento, identificar brechas e incidentes de seguridad, y comprobar si las acciones tomadas para resolver incidentes de seguridad han sido eficaces.
- Revisar regularmente la eficacia del SGSI: en función de los resultados de auditorías de seguridad.
- Medir la eficacia de los controles.
- Revisar regularmente la evaluación de riesgos: influencian los cambios en la organización, tecnología, procesos y objetivos de negocio, amenazas, eficacia de los controles o el entorno.
- Realizar regularmente auditorías internas: para determinar si los controles, procesos y procedimientos del SGSI mantienen la conformidad con los requisitos de ISO 27001.
- Revisar regularmente el SGSI por parte de la Dirección.
- Actualizar planes de seguridad: teniendo en cuenta los resultados de la monitorización y las revisiones.
- Registrar acciones y eventos que puedan tener impacto en la eficacia o el rendimiento del SGSI.

3.1.6.4 MEJORA CONTINÚA (ACTUAR)

Ilustración 3. 4 Fase Actuar

- Implantar mejoras: poner en marcha todas las mejoras que se hayan propuesto en la fase anterior.
- Acciones correctivas: para solucionar no conformidades detectadas.
- Acciones preventivas: para prevenir potenciales no conformidades.
- Comunicar las acciones y mejoras: a todos los interesados y con el nivel adecuado de detalle.
- Asegurarse de que las mejoras alcanzan los objetivos pretendidos: la eficacia de cualquier acción, medida o cambio debe comprobarse siempre.

3.1.7 Sistema de Gestión de Seguridad de la Información (SGSI)

El Sistema de Gestión de Seguridad de la Información es el concepto central sobre el que se construye ISO 27001. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. Este proceso es el que constituye un SGSI, que podría considerarse, como el sistema de calidad para la seguridad de la información. Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

3.1.8 ISO 27002

ISO/IEC 27002 es un estándar para la seguridad de la información publicado por primera vez como ISO/IEC 17799:2000 por la ISO e IEC en el año 2000. Tras un periodo de revisión y actualización de los contenidos del estándar, se publicó en el año 2005 el documento actualizado denominado ISO/IEC 17799:2005.

ISO/IEC 27002 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)".
La versión de 2005 del estándar incluye las siguientes once secciones[6] principales:

1. Política de Seguridad de la Información.
2. Organización de la Seguridad de la Información.
3. Gestión de Activos de Información.
4. Seguridad de los Recursos Humanos.
5. Seguridad Física y Ambiental.
6. Gestión de las Comunicaciones y Operaciones.
7. Control de Accesos.
8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.

[6] Revisar Anexo 1: Definiciones y Términos

9. Gestión de Incidentes en la Seguridad de la Información.
10. Gestión de Continuidad del Negocio.
11. Cumplimiento.

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información. Para cada uno de los controles se indica, asimismo, una guía para su implantación.

3.2 Políticas de la Empresa ACB INGENIERIA S.A., aplicadas a Recursos Humanos

3.2.1 Reclutamiento, selección e ingreso de personal

POLÍTICA

Toda creación de un nuevo puesto y/o cargo, debe ser aprobado por el Gerente, previo al inicio de cualquier proceso de reclutamiento.

3.2.2 Capacitación de personal

POLÍTICA

Se promueve la capacitación del personal, con énfasis el entrenamiento interno y continuo que cada Jefe de área debe dar.

3.2.3 Calificación de personal

POLÍTICA

Definir la forma de calificar el personal que labora en la empresa.

3.2.4 Transporte y Alimentación

POLÍTICA

Normar el pago que por concepto de movilización y alimentación que se debe efectuar a los colaboradores que por motivo de trabajo deban permanecer en la institución. No aplica a Gerentes.

CAPÍTULO 4
ANÁLISIS DE RIESGO

4. Análisis de Riesgo

4.1 Valoración de Activos

La valoración de activos comprende el proceso de determinación de activos, establecimiento de las amenazas sobre los activos y cálculo del impacto a partir de varias escalas de valoración.

4.1.1 Determinación de Activos:

Los activos que intervienen en el área de Recursos Humanos de la empresa ACB INGENIERIA S.A. son los siguientes:

Tipo de Activo	Activo
Servicios	Servicio de Internet Correo Electrónico Interno Gestión de Identidades Help Desk
Datos	Datos de Gestión Interna Datos de Carácter Personal
Aplicaciones	Software Utilitario Sistemas Operativos Navegador Web Sistema de Backup – Open KM Antivirus
Equipos Informáticos	Informática Personal Periféricos Soporte de Red
Redes de Comunicaciones	Central Telefónica Equipos de Acceso a Internet
Personal	Área Gestión de Calidad Área Dirección Área Compensación y Liquidación Área Custodia y Ejercicio de Derecho Área Gestión de Cobro y Libro de Acciones Área Sistemas Área Administrativa y Recursos Humanos Área Contabilidad Área Legal

Tabla 4. 1 Determinación de Activos

4.1.2 Ponderación de la Dimensiones de los Activos:

Los activos enlistados serán ponderados en base a la escala correspondiente[7]. Las dimensiones referenciadas son Confiabilidad, Integridad y Disponibilidad. A continuación, se detalla los activos y se estipula la ponderación de las dimensiones según el levantamiento de información:

Activo: Servicio	Disponibilidad	Confiabilidad	Integridad	Total
Servicio de Internet	5	4	4	13
Correo Electrónico Interno	5	4	5	14
Gestión de Identidades	5	5	5	15

Tabla 4. 2 Ponderación de las Dimensiones de Activo Servicio

Activo: Datos	Disponibilidad	Confiabilidad	Integridad	Total
Datos de Gestión Interna	5	5	4	14
Datos de Carácter Personal	5	3	3	11

Tabla 4. 3 Ponderación de las Dimensiones de Activo Datos

Activo: Aplicaciones	Disponibilidad	Confiabilidad	Integridad	Total
Software Utilitario	5	4	4	13
Sistema Operativo	5	4	3	12
Navegador Web	3	3	3	9
Sistema Backup OPEN KM	4	5	5	14
Antivirus	4	4	4	12

Tabla 4. 4 Ponderación de las Dimensiones de Activo Aplicaciones

Activo: Equipos Informáticos	Disponibilidad	Confiabilidad	Integridad	Total
Informática Personal	5	4	4	13
Periféricos	5	4	3	12
Soporte de Red	5	4	4	13

Tabla 4. 5 Ponderación de las Dimensiones de Activo Equipos Informáticos

Activo: Redes de Comunicaciones	Disponibilidad	Confiabilidad	Integridad	Total
Central Telefónica	5	5	4	14
Equipo de Acceso a Internet	5	5	5	15

[7] Revisar Anexo 5: Escala de Valoración de los Activos

Tabla 4. 6 Ponderación de las Dimensiones de Activo Redes de Comunicaciones

Activo: Personal	Disponibilidad	Confiabilidad	Integridad	Total
Área Gestión de Calidad	5	5	5	15
Área Dirección	5	5	5	15
Área Compensación y Liquidación	5	5	5	15
Área Custodia y Ejercicio de Derecho	5	5	5	15
Área Gestión de Cobro y Libro de Acciones	5	5	5	15
Área Sistemas	4	5	4	15
Área Administrativa y Recursos Humanos	5	5	5	15
Área Contabilidad	5	5	5	15
Área Legal	4	5	4	15

Tabla 4. 7 Ponderación de las Dimensiones de Activo Personal

4.1.3 Determinación de las Amenazas por Activo:

Activo: Servicio	Amenazas
Servicio de Internet	Uso inapropiado Acceso no autorizado Falta de servicio Interferencia
Correo Electrónico Interno	Usurpación de identidad Falta de servicio Acceso no autorizado Reencaminamiento de mensajes Uso no previsto
Gestión de Identidades	Uso no previsto Manipulación de la credencial de acceso Falta de energía eléctrica Manipulación de la configuración del aplicativo Usurpación de identidad Robo o perdida de la credencial de acceso

Tabla 4. 8 Determinación de Amenazas Activo Servicio

Activo: Datos	Amenazas
Datos de Gestión Interna	Alteración de la información

	Destrucción de la información Cambio de ubicación de la información Conocimiento no autorizado Manipulación de la configuración Divulgación de la información
Datos de Carácter Personal	Errores de los usuarios Acceso no autorizado Conocimiento no autorizado Destrucción de la información Degradación de la información Divulgación de la información

Tabla 4. 9 Determinación de Amenazas Activo Datos

Activo: Aplicaciones	Amenazas
Software Utilitario	Ataque de virus Manipulación de programas Errores de usuario
Sistema Operativo	Suplantación de la identidad de usuario Errores de administración Propagación de software malicioso Acceso no autorizado
Navegador Web	Abuso de privilegio de acceso Manipulación de configuración de red Manipulación de programas
Sistema Backup OPEN KM	Suplantación de la identidad de usuario Manipulación de programas Caída del servidor web Open KM Errores de usuario
Antivirus	Desactualización de antivirus Errores de administración Manipulación de programas

Tabla 4. 10 Determinación de Amenazas Activo Aplicaciones

Activo: Equipos Informáticos	Amenazas
Informática Personal	Acceso no autorizado Modificación de la asignación del equipo Accidentes imprevistos Falta de energía eléctrica Manipulación de las propiedades del equipo Ingreso no autorizado del equipo
Periféricos	Acceso no autorizado Accidentes imprevistos Cambio de ubicación no autorizado
Soporte de Red	Manipulación de la configuración de red Errores de administración Falta de energía eléctrica Ausencia de puntos de red

Tabla 4. 11 Determinación de Amenazas Activo Equipos Informáticos

Activo: Redes de Comunicaciones	Amenazas
Central Telefónica	Manipulación de la asignación de las Ips Falta de energía eléctrica Accidentes imprevistos Caída del servidor de la central telefónica
Equipo de Acceso a Internet	Manipulación de la configuración Accidentes imprevistos Caída del servidor proveedor Problemas con las conexiones del proveedor Errores de administración Falta de energía eléctrica

Tabla 4. 12 Determinación de Amenazas Activo Redes de Comunicaciones

Activo: Personal	Amenazas
Área Gestión de Calidad Área Dirección Área Compensación y Liquidación Área Custodia y Ejercicio de Derecho Área Gestión de Cobro y Libro de Acciones Área Sistemas Área Administrativa y Recursos Humanos Área Contabilidad Área Legal	Desconocimiento de sus funciones Mala organización Indisponibilidad del personal Divulgación de la información Extorsión Manipulación de la información Destrucción de la información

Tabla 4. 13 Determinación de Amenazas Activo Personal

4.1.4 Cálculo de riesgo:

A partir del levantamiento de información, donde se arrojo el nivel de frecuencia e impacto[8] al activo mediante la amenaza se han calculado los riesgos por cada una:

Activo	Amenazas	Frecuencia	Impacto	Total
Servicio de Internet	Uso inapropiado	3	3	9
	Acceso no autorizado	2	4	8
	Falta de servicio	1	5	5
	Interferencia	2	4	8
Correo Electrónico Interno	Usurpación de identidad	2	4	8
	Falta de servicio	1	4	4
	Acceso no autorizado	4	3	12

[8]Revisar Anexo 5: Escala de Valoración de Activos

	Reencaminamiento de mensajes	4	3	12
	Uso no previsto	3	3	9
Gestión de Identidades	Uso no previsto	2	4	8
	Manipulación de la credencial de acceso	3	5	15
	Falta de energía eléctrica	4	2	8
	Manipulación de la configuración del aplicativo	2	2	4
	Usurpación de identidad	3	4	12
	Robo o perdida de la credencial de acceso	4	5	20
Datos de Gestión Interna	Alteración de la información	2	5	10
	Destrucción de la información	3	5	15
	Manipulación de la configuración	2	5	10
	Divulgación de información	4	4	16
Datos de Carácter Personal	Errores de los usuarios	4	4	16
	Acceso no autorizado	3	3	9
	Destrucción de información	2	5	10
	Degradación de la información	2	5	10
	Divulgación de información	2	3	6
Software Utilitarios	Ataque de virus	2	2	4
	Manipulación de programas	3	2	6
	Errores de usuario	4	4	16
Sistemas Operativos	Suplantación de identidad de usuario	3	3	9
	Errores de administración	3	4	12
	Propagación de software malicioso	2	3	6
	Acceso no autorizado	3	4	12
Navegador Web	Abuso de privilegios de acceso	4	3	12
	Manipulación de configuración de red	2	3	6
	Manipulación de programas	2	2	4
Sistema de BackUp	Manipulación de programas	2	2	4

Open KM	Suplantación de identidad de usuario	2	2	4
	Caída del servidor web Open KM	2	2	4
	Errores de usuario	3	2	6
Antivirus	Desactualización de antivirus	1	2	2
	Errores de administración	2	2	4
	Manipulación de programas	2	2	4
Informática Personal	Acceso no autorizado	3	2	6
	Modificación de la asignación del equipo	3	2	6
	Accidentes imprevistos	3	2	6
	Falta de energía eléctrica	3	2	6
	Manipulación de las propiedades del equipo	3	2	6
	Ingreso no autorizado de equipo	2	3	6
Periféricos Impresoras Scanners	Acceso no autorizado	5	3	15
	Accidentes imprevistos	4	3	12
	Cambio de ubicación no autorizado	3	3	9
Soporte de Red	Manipulación de configuración de red	2	4	8
	Errores de administración	2	4	8
	Falta de energía eléctrica	4	5	20
	Ausencia de puntos de red	4	4	16
Central Telefónica	Manipulación de asignación de Ips	2	4	8
	Falta de energía eléctrica	3	5	15
	Accidentes imprevistos	3	3	9
	Caída del servidor de la central telefónica	4	4	16
Equipo de Acceso a Internet	Manipulación de configuración	2	4	8
	Accidentes imprevistos	2	4	8

	Caída del servidor proveedor	2	4	8
	Problemas con las conexiones del proveedor	2	4	8
	Errores de administración	2	4	8
	Falta de energía eléctrica	3	5	15
Personal: Diferentes áreas	Desconocimientos de sus funciones	4	4	16
	Mala organización	3	3	9
	Indisponibilidad del personal	2	2	4
	Divulgación de información	3	3	9
	Extorsión	3	2	6
	Manipular información	4	4	16
	Destruir información	4	4	16

Tabla 4. 14 Resultado del Cálculo de Riesgo de los Activos

4.2 Plan de tratamiento de riesgo

ACTIVOS	AMENAZAS	VULNERABILIDADES	PTR
Servicio de Internet	Uso inapropiado	No respetar los límites de acceso Falta de capacitación sobre los límites de acceso	Aceptar Reducir
	Acceso no autorizado	No respetar los límites de acceso	Aceptar
	Falta de servicio	Problemas del proveedor de internet	Transferir
	Interferencia	Falta de protección de la red	Aceptar
Correo Electrónico Interno	Usurpación de identidad	Falta de control en el acceso Divulgación de la información de acceso	Reducir Reducir
	Falta de servicio	Falta del servicio de Internet Interferencia con el servidor interno de correo	Transferir Reducir
	Acceso no autorizado	No respetar los límites de acceso Usurpación de identidad	Aceptar Reducir

	Reencaminamiento de mensajes	Falta de seguridad en la transferencia de mensajes	Aceptar
	Uso no previsto	Falta de políticas	Reducir
Gestión de Identidades	Uso no previsto	Falta de políticas	Reducir
	Manipulación de la credencial de acceso	Falta de implementación de mayor seguridades en la credencial	Reducir
	Falta de energía eléctrica	Falta de generador eléctrico	Aceptar
	Manipulación de la configuración del aplicativo	Falta de políticas	Reducir
	Usurpación de identidad	Falta de control en el acceso	Reducir
	Robo o perdida de la credencial de acceso	Falta de método de apoyo para el caso	Reducir
Datos de Gestión Interna	Alteración de la información	Insuficiente entrenamiento de empleados	Reducir
	Destrucción de la información	Falta de un debido control de acceso a usuarios y de una protección física	Reducir
	Cambio de ubicación de la información	Falta de protección física adecuada	Reducir
	Manipulación de la configuración	Falta de un debido control de acceso a usuarios	Reducir
	Divulgación de la información	Almacenamiento no protegido	Reducir
	Errores de los usuarios	Falta de conocimiento y oportuno entrenamiento	Reducir
Datos de Carácter Personal	Acceso no autorizado	Falta de políticas y protección física	Reducir
	Destrucción de la información	Falta de un debido control de acceso a usuarios y de una protección física	Reducir
	Degradación de la información	Falta de mantenimiento adecuado	Reducir
	Divulgación de la información	Almacenamiento no protegido	Aceptar
	Ataque de virus	Falta de protección contra aplicaciones dañinas	Aceptar
	Manipulación de programas	Insuficiente entrenamiento de empleados	Aceptar
Software Utilitario	Errores de usuario	Falta de conocimiento y oportuno entrenamiento	Reducir
	Suplantación de la identidad de usuario	Falta de control de acceso	Aceptar

	Errores de administración	Falta de conocimiento de funciones del administrador	Reducir
Sistema Operativo	Propagación de software malicioso	Falta de protección y controles en las configuraciones de la red	Aceptar
	Acceso no autorizado	Falta de políticas y protección física	Reducir
	Abuso de privilegio de acceso	Falta de conocimiento y oportuno entrenamiento	Reducir
	Manipulación de configuración de red	Falta de control de acceso	Aceptar
Navegador Web	Manipulación de programas	Insuficiente entrenamiento de empleados	Aceptar
	Suplantación de la identidad de usuario	Falta de control de acceso	Aceptar
	Caída del servidor web Open KM	Instalación de SW no Autorizado	Aceptar
Sistema Backup OPEN KM	Errores de usuario	Falta de conocimiento y oportuno entrenamiento	Aceptar
	Desactualización de antivirus	Falla del servicio de red	Aceptar
	Errores de administración	Falta de conocimiento de funciones del administrador	Reducir
	Manipulación de programas	Insuficiente entrenamiento de empleados	Aceptar
Antivirus	Acceso no autorizado	Falta de políticas	Reducir
	Modificación de la asignación del equipo	Falta de control de Acceso	Aceptar
	Accidentes imprevistos	Condiciones locales donde los recursos son fácilmente afectados	Reducir
Informática Personal	Falta de energía eléctrica	Falta de acuerdos bien definidos con terceras partes	Aceptar
	Manipulación de las propiedades del equipo	Falta de control de acceso	Aceptar
	Ingreso no autorizado del equipo	Falta de control de acceso	Aceptar
	Acceso no autorizado	Falta de control de acceso	Reducir
	Accidentes imprevistos	Condiciones locales donde los recursos son fácilmente afectados	Reducir
	Cambio de ubicación no autorizado	Falta de protección física adecuada	Aceptar

Periféricos	Manipulación de la configuración de red	Falta de control de seguridad	Aceptar
	Errores de administración	Falta de conocimiento de funciones del administrador	Reducir
	Falta de energía eléctrica	Falta de acuerdos bien definidos con terceras partes	Reducir
Soporte de Red	Ausencia de puntos de red	Capacidad insuficiente de los recursos	Reducir
	Manipulación de la asignación de las Ips	Falta de control de acceso	Aceptar
	Falta de energía eléctrica	Falta de acuerdos bien definidos con terceras partes	Reducir
	Accidentes imprevistos	Condiciones locales donde los recursos son fácilmente afectados	Reducir
Central Telefónica	Caída del servidor de la central telefónica	Falta de acuerdos bien definidos con terceras partes	Reducir
	Manipulación de la configuración	Falta de control de acceso	Aceptar
	Accidentes imprevistos	Condiciones locales donde los recursos son fácilmente afectados	Reducir
	Caída del servidor proveedor	Falta de acuerdos bien definidos con terceras partes	Transferir
Equipo de Acceso a Internet	Problemas con las conexiones del proveedor	Falta de acuerdos bien definidos con terceras partes	Transferir
	Errores de administración	Falta de conocimiento de funciones del administrador	Reducir
	Falta de energía eléctrica	Falta de capacitación del administrador	Reducir
	Desconocimiento de sus funciones	Falta de conocimiento y oportuno entrenamiento	Reducir
	Mala organización	Desconocimiento de estándares y reglas establecidas por la empresa Falta de reglas según el caso	Reducir
	Indisponibilidad del personal	Falta de conocimiento y oportuno entrenamiento	Aceptar
Recursos Humanos	Divulgación de la información	Almacenamiento no protegido	Reducir
	Extorsión	Desconocimiento de estándares y reglas establecidas por la empresa Falta de reglas según el caso	Reducir

	Manipulación de la información	Insuficiente entrenamiento de empleados	Reducir
	Destrucción de la información	Falta de un debido control de acceso a usuarios y de una protección física	Reducir
	Falla en la elección del personal	Falta de especificaciones con respecto a la selección de personal	Reducir

Tabla 4. 15 Plan de Tratamiento de Riesgo

4.3 Declaración de Aplicación

A continuación, se detallara la Declaración de Aplicación (SOA) para determinar las responsabilidades del control a realizar a través del sistema de gestión de seguridad de la información:

ISO 27001: 2005 Controles			Controles Utilizados	Observaciones (Justificación de exclusión)	Controles seleccionados y las razones para la selección				Observaciones (Descripción general de la aplicación)
					LR	CO	BR/BP	RRA	
Clausula	Sec.	Objetivo de control/Controles							
Seguridad de los Recursos Humanos	8.1	Antes del Empleo							
	8.1.1	Roles y Responsabilidades		Controles desarrollados por otra ISO					
	8.1.2	Detección		Controles desarrollados por otra ISO					
	8.1.3	Términos y condiciones del empleado		Controles desarrollados por otra ISO					
	8.2	Durante el Empleo							
	8.2.1	Responsabilidad de la Dirección	X			X	X		Se debe detallar los procedimientos para controlar que las políticas de seguridad de la empresa se estén aplicando en las labores diarias.
	8.2.2	Formación y capacitación en seguridad de la información	X				X	X	Definir las actividades a realizar para aplicar el control y transmitir las políticas de seguridad o actualizaciones de las mismas.

	8.2.3	Comunicación de eventos y debilidades de la seguridad de la información	X				X	X	Se debe estructurar un procedimiento a seguir en caso de que alguna política sea infringida por los usuarios.
	8.3	Terminación y Cambio de Empleo							
	8.3.1	Terminación de las responsabilidades		Desarrollado por otro grupo					
	8.3.2	Restitución de activos		Desarrollado por otro grupo					
	8.3.3	Remover los permisos de acceso		Desarrollado por otro grupo					

Tabla 4. 16 Declaración de Aplicabilidad

CAPÍTULO 5
ETAPA 2: HACER

5. Etapa 2: Hacer

5.1 Alcance y Límites de la Gestión de Seguridad

El Sistema de Gestión de Seguridad de la Información aplicado al área de Recursos Humanos de la empresa ACB INGENIERIA S.A., se desea implementar en la siguiente área:
Área Seguridad en el desempeño de las funciones del empleo (Durante el empleo):

Objetivos:

- Asegurar que los empleados, contratistas y terceras partes son conscientes de las amenazas de seguridad, de sus responsabilidades y obligaciones y que están equipados para cumplir con la política de seguridad de la organización en el desempeño de sus labores diarias, para reducir el riesgo asociado a los errores humanos.

5.1.1 Control: Supervisión de las obligaciones

Descripción: La Dirección debería requerir a empleados, contratistas y usuarios de terceras partes aplicar la seguridad en concordancia con las políticas y los procedimientos establecidos de la organización.

5.1.2 Control: Formación y capacitación en seguridad de la información

Descripción: Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.

5.1.3 Control: Procedimiento disciplinario

Descripción: Debería existir un proceso formal disciplinario para empleados que produzcan brechas en la seguridad.

5.2 Objetivos

5.2.1 Objetivo General:

Efectuar un sistema de gestión de seguridad de la información correspondiente al área de recursos humanos para mejorar los procesos de capacitación y formación de seguridad de información y demostración del aplicar el conocimiento transmitido, mediante el establecimiento de procedimientos y lineamientos referentes al tema ajustados a controles de actualización.

5.2.2 Objetivos Específicos:

- Establecer y documentar los procedimientos a seguir para realizar la capacitación de las políticas de seguridad de información que posee la empresa.
- Definir los lineamientos de introducción del personal a las tecnologías de la empresa.
- Desarrollar controles que permite verificar que las seguridades de la organización están siendo utilizadas dentro de sus procesos.
- Implementar procesos para actualización de los posibles cambios de las políticas de seguridad de la información.
- Desarrollar los procedimientos debidos para control y resguardo del flujo de la información de recursos humanos.
- Crear una conciencia de seguridad aplicable a los activos de información.
- Reducir el riesgo de robo, fraude y mal uso de los medios a través de información vigente, de conocimiento público y la conciencia de seguridad dentro de la empresa.
- Determinar procedimientos disciplinarios que permitan sancionar a todo aquel que infrinja alguna de las políticas de seguridad implementadas.
- Establecer una metodología de gestión de la seguridad clara y estructurada.
- Accesar a la información a través medidas de seguridad, por parte de los usuarios.
- Revisar continuamente, los controles implementados por la gestión realizada.
- Crear un ambiente de confianza y reglas claras dentro de la compañía, con respecto a la seguridad de información que manipulan y corresponde al área gestionada.
- Brindar la posibilidad de integrarse con otros sistemas de gestión y certificar.
- Minimizar la paralización de las operaciones de negocio por incidentes de gravedad.
- Mantener y mejorar la imagen de confiabilidad y seguridad de la empresa, siendo elemento diferenciador de la competencia.

Todos estos propósitos tienen la finalidad de cumplir el general, desarrollando el sistema de gestión indicado para disminuir el número de amenazas que pueden someter a activos de información a diversas formas de fraude, sabotaje o vandalismo. En área donde se desea aplicar la gestión de seguridad permitirá entre tanto que las amenazas referentes al personal sean conocidas y reducidas.

5.3Definición de Políticas de Seguridad

5.3.1 Políticas de Confiabilidad

La gestión a desarrollar indica los siguientes parámetros para mantener la confiabilidad de la información:

- Todo cambio dentro de la información del sistema debe ser notificada vía escrita firmada por el jefe de departamento que comunica el cambio, directamente, al encargado del área de sistemas.
- La información a ingresar debe ser correctamente revisada, y teniendo en cuenta que los datos manejados son de vital importancia para el desempeño de las funciones de la compañía y aun más relevantes para los clientes de la misma.
- La eliminación de la información no es permitida, solamente se pueden realizar registros nuevos con la modificación.

5.3.2 Políticas de integridad

Se sugiere a la compañía seguir los siguientes lineamientos para mantener la integridad de su información:

- Cada acceso al sistema deber mediante nombre de usuario y clave.
- El nombre de usuario y clave será dado al momento de la incorporación a la empresa.
- En caso de cambio de los datos de acceso, deberá ser notificado por escrito, detallando la causa del cambio y firmado por el responsable y el jefe del departamento de recursos humanos. Los cambios de cargo, sueldo, carga familiar, etc. se podrán realizar directamente en el sistema asignado al área de recursos humanos.
- En caso de finalización de la relación laboral, deberá ser notificado por escrito, detallando la causa y firmado por el responsable y el jefe del departamento de recursos humanos. El cambio cambiará el estado de la información de acceso a inactivado. Una vez inactivado esta información no podrá ser cambiado a ningún otro estado.
- Al intentar ingresar al sistema, solo se podrá escribir la clave hasta cinco veces. Al completar el limite, el usuario de bloqueará.
- El bloqueo de un usuario solo podrá ser inhabilitado, mediante un oficio escrito donde se detalle la causa del bloqueo firmado por el responsable y el jefe del departamento referido. Este documento debe ser entregado al encargado del área de sistemas.
- La información de acceso es responsabilidad, totalmente, del empleado a la cual fue asignada y no debe ser divulgada a ningún tercero.
- La información de acceso es considerada de carácter secreto e intransferible.

5.3.3 Políticas de disponibilidad

Las políticas de disponibilidad detallan las especificaciones para mantener la información correcta para quienes la puedan consultar:

- El ingreso o modificación de la información del sistema será un proceso en línea.
- La información de los clientes es considerada de carácter privado.
- En caso de modificación de la información del sistema, el registro o los registros utilizados serán bloqueados para evitar error en el cambio de los datos.

5.3.4 Políticas de manejo de Recursos Humanos (Durante el Empleo)

- La compañía debe mantener un buen ambiente de trabajo dentro de la misma, promoviendo la vinculación integral entre las áreas de trabajo y personal en general.
- La empresa determina los principios del cumplimiento de las disposiciones que norman las conductas a seguir para lograr los resultados buscados, dentro de un clima de trabajo positivo y ajustarlo a la aplicación de una justa retribución.
- La compañía debe entrenar, capacitar y actualizar al personal en las políticas y procedimientos de seguridad que prevén proteger los activos de información.
- El personal de la empresa debe estar siempre presto a la capacitación de las políticas y procedimientos de seguridad para evitar realizar infracciones o violaciones de los mismos.

- La compañía debe publicar, periódicamente, el listado de infracciones o violaciones de políticas de seguridad.
- El personal de la empresa debe conocer los procedimientos disciplinarios a seguir en caso de infracción o violación de las políticas de seguridad.
- La empresa determina los lineamientos de verificación de aplicabilidad de las políticas y procedimientos de seguridad de la información.

5.5 Procedimientos según el sistema de gestión:

5.5.1 Procedimiento para verificar que las políticas y procedimientos de seguridad de la información están siendo aplicados

5.5.1.1 Objetivo

Verificar que las políticas y procedimientos de seguridad de información instalados en la empresa estén siendo aplicados y mediante los mismos se mantenga el desenvolvimiento de la empresa.

5.5.1.2 Alcance

La Dirección debería requerir a empleados, contratistas y usuarios de terceras partes aplicar la seguridad en concordancia con las políticas y los procedimientos establecidos de la organización. La aplicación y cumplimiento de éste procedimiento es responsabilidad del departamento de Recursos Humanos.

5.5.1.3 Responsabilidades

De los *Gerentes* junto con la *Jefe Nacional Administrativa*: Definir los lineamientos de aplicabilidad de las políticas y procedimientos de seguridad.

Del *Jefe de cada Área:* Realizar la aplicación del formulario de aplicabilidad de políticas de seguridad[9]. Los formularios completados deben ser remitidos a la Jefe Nacional Administrativa.

De la *Jefe Nacional Administrativa*: Revisar el formulario de aplicabilidad de políticas de seguridad, para generar un informe de observaciones. De encontrar alguna anomalía, se registra en el formulario de registro de inconformidad[10]. Los documentos generados deben ser remitidos a los Gerentes. Aplicar alguna sanción según la infracción realizada y la anotación de los Gerentes.
De *los Gerentes*: Revisar los informes enviados por la Jefe Nacional Administrativa y realizar anotaciones por cualquier índole.

[9] Revisar Anexo 6: Formulario de Aplicabilidad de las Políticas de Seguridad
[10] Revisar Anexo 7: Registro de Inconformidades

5.5.1.4 Descripción del Procedimiento

Necesidades de Verificación de Aplicabilidad de Seguridades.-

Las razones por la cuales se podría considerar que se necesite de realizar verificación de la aplicabilidad de las políticas y procedimientos de seguridad son:

- Infringir alguna de las políticas de seguridad que cree dificultades graves dentro de la organización.
- Seguimiento de la aplicabilidad de las seguridades.
- Cumplir el seguimiento a la aplicabilidad de las políticas y procedimientos de seguridad.
- Sugerencias de los empleados.

Cualquier requerimiento para verificación de aplicabilidad del personal puede ser canalizado por escrito.

Plan de Verificación de Aplicabilidad de Seguridades

La Jefe Nacional Administrativa

- Al inicio de cada año elabora el "Plan de Verificación de Aplicabilidad de Seguridades" en la planilla correspondiente al plan a elaborar[11], el cual debe ser aprobado por la Gerencia.
- En caso de que se hubieran detectado Necesidades de Verificaciones de Aplicabilidad por cualquiera de los puntos indicados, estas deben ser consideradas por "Actualización del Plan de Verificación de Aplicabilidad de Seguridades".
- El Plan de Verificación de Aplicabilidad prevé aplicar el formulario de verificación de aplicabilidad de las políticas de seguridad[12] que incluye serie de preguntas acerca de las seguridades implementadas en la empresa y como es aplicada por el cuestionado.

Los empleados

Serán informados sobre la ejecución del Plan de Verificación de Aplicabilidad mediante un boletín de información[13] publicado en la cartelera de la empresa.

- No se permitirán faltas ni atraso durante la ejecución del Plan de Verificación, sin importancia de índoles. Cualquier empleado que no cumpla con lo estipulado, será considerado para sanción, según procedimientos disciplinarios.

Actualización del Plan de Verificación de Aplicabilidad de Seguridades

[11] Revisar Anexo 8: Plan de Verificación de Aplicabilidad de Seguridades
[12] Revisar Anexo 6: Formulario de Verificación de Aplicabilidad de Seguridades
[13] Revisar Anexo 9: Boletín de información: Plan de Verificación de Aplicabilidad

Si se presentan actividades que se consideren como necesidades de verificación de aplicabilidad adicionales a las previstas en el Plan de Verificación de Aplicabilidad, estas se ingresarán mediante solicitud escrita. Dicha verificación de aplicabilidad deberá ser aprobada por la Gerencia.

La Jefe Nacional Administrativa

- Analiza la solicitud y determina la logística, presupuesto, costos y posible cronograma. Toda esta información la remite a la Gerencia quien da su aprobación.
- Si la verificación de aplicabilidad es aprobada, es incluida en el Plan de Verificación de Aplicabilidad de Seguridades.
- Los incumplimientos al "Plan de Verificación de Aplicabilidad de Seguridades" deberán ser justificados en el mismo formato, columna Justificación de incumplimiento. En dicha columna se debe registrar la causa de la falta.

Control de Asistencia de Ejecución de Verificación de Aplicabilidad

La Jefe Nacional Administrativa

- Se estructura un formulario de registro de asistencia a ejecución de verificación de aplicabilidad[14].
- Una vez que la verificación de aplicabilidad ha sido terminada, se archiva el registro de asistencia de la misma.

5.5.2 Procedimiento para capacitar sobre las políticas y procedimientos de seguridad de la información y sus actualizaciones

5.5.2.1 Objetivo

Comunicar las políticas y procedimientos de seguridad de información instalados en la empresa, a través de capacitaciones pertinentes para ser aplicadas en el desarrollo de las actividades diarias.

5.5.2.2 Alcance

La Dirección debería capacitar a empleados, contratistas y usuarios de terceras partes acerca de la seguridad en concordancia con las políticas y los procedimientos establecidos de la organización. La aplicación y cumplimiento de éste procedimiento es responsabilidad del departamento de Recursos Humanos.

5.5.2.3 Responsabilidades

De los ***Gerentes*** junto con la ***Jefe Nacional Administrativa***: Definir el "Plan de Capacitación: Seguridad de la Información".

[14] Revisar Anexo 11: Formulario de Control de Asistencia de Verificación de Aplicabilidad

De la *Jefe Nacional Administrativa*: de coordinar la ejecución de las actividades de capacitación del personal que lo necesite y de hacer seguimiento al cumplimiento del Plan de Capacitación.

5.5.2.4 Descripción del Procedimiento

Necesidades de Capacitación

Las razones por la cuales se podría considerar que se necesite de capacitación son:

- Infringir alguna de las políticas de seguridad por desconocimiento de la misma.
- Desarrollar conciencia con respecto a la seguridad de la información.
- Calificación del personal que indique necesidad de capacitación.
- Capacitación organizada por requerimiento de la Jefe Nacional Administrativa.
- Se considera que los empleados desconocen sobre las políticas y los procedimientos de seguridad.
- Sugerencias de los empleados.

Cualquier requerimiento para capacitación del personal debe ser canalizado por escrito.

Plan de Capacitación: Seguridad de la Información

La Jefe Nacional Administrativa

- Al inicio de cada año elabora el "Plan de Capacitación: Seguridad de Información" en la planilla correspondiente al plan a elaborar[15], el cual debe ser aprobado por la Gerencia.
- En caso de que se hubieran detectado Necesidades de Capacitación por cualquiera de los puntos indicados, estas deben ser consideradas para "Actualización del Plan de Capacitación: Seguridad de la Información".
- El Plan de Capacitación incluye la información referente a: tema, participantes, horas, y fechas aproximadas.

Los empleados

- Serán informados del inicio de una capacitación con un tiempo prudente, mediante carta de convocatoria[16].
- No se permitirán faltas ni atraso para ninguna capacitación, sin importancia de índoles, siempre y cuando el empleado haya sido convocado.

Actualización del Plan de Capacitación: Seguridad de la Información

Si se presentan actividades de capacitación adicionales a las previstas en el Plan de Capacitación, estas se ingresarán mediante solicitud escrita. Dicha capacitación deberá ser aprobada por la Gerencia. Esto se aplica principalmente cuando se requiere de capacitaciones externas.

La Jefe Nacional Administrativa

- Analiza la solicitud y determina la logística, presupuesto, costos y posible cronograma. Toda esta información la remite a la Gerencia quien da su aprobación.

[15] Revisar Anexo 12: Planilla de Plan de Capacitación: Seguridad de la Información
[16] Revisar Anexo 13: Carta de convocatoria a empleados.

- Si la capacitación es aprobada, es incluida en el Plan de Capacitación.
- Los incumplimientos al "Plan de Capacitación: Seguridad de la información" deberán ser justificados en el mismo formato, columna Justificación de incumplimiento. En dicha columna se debe registrar la causa de la falta.

Control de Asistencia a Capacitación

La Jefe Nacional Administrativa

- Se estructura un formulario de registro de asistencia a capacitación[17]. Si la capacitación es externa, se debe entregar un formulario similar a cargo de uno de los enviados y deberá ser firmada por los empleados de la compañía.
- Una vez que la capacitación ha sido terminada, se archiva el registro de asistencia de la misma.

Certificado de la Capacitación

- Los certificados de capacitación serán entregados en mismo día en que la misma será terminada. Se archiva una copia del certificado en la carpeta de personal.
- Si la capacitación ha sido externa, el certificado será entregado según la entidad externa. De igual manera, se archiva una copia del certificado en la carpeta de personal.

5.5.3 Procedimiento para aplicar sanciones por infracción sobre alguna política de seguridad de la empresa.

5.5.3.1 Objetivo

Aplicar sanciones por infracción o violación de alguna política de seguridad que rige en la empresa,por parte del personal que ha sido capacitado, a través, de distintos procedimientos disciplinarios.

5.5.3.2 Alcance

Debería existir un proceso formal disciplinario para empleados que produzcan brechas en la seguridad.

5.5.3.3 Responsabilidades

De los ***Gerentes*** junto con la ***Jefe Nacional Administrativa***: Definir los procedimientos disciplinarios que se aplicaran por infracción o violación de alguna política de seguridad.
De la ***Jefe Nacional Administrativa***: de aplicar el procedimiento disciplinario correspondiente a la infracción o violación realizada. Comunicar a los empleados de dichos procedimientos disciplinarios, valiéndose del Plan de Capacitación: Políticas de Seguridad.

[17] Revisar Anexo 14: Formulario de Control de Asistencia a Capacitación

5.5.3.4 Descripción del Procedimiento

Tipos de Infracciones o Violaciones a las Políticas de Seguridad.-
Algunos tipos de infracción o violaciones a las políticas de seguridad por la cuales se podría considerar aplicar procedimiento disciplinario son:

- Alteración, destrucción, divulgación y cambio de ubicación de información (Dentro y fuera de la compañía).
- Uso inapropiado de los diferentes recursos (Acceso no autorizado).
- Usurpación de identidad
- Manipulación de credenciales de acceso (Ingreso del trabajo)
- Manipulación de la configuración de los aplicativos de las estaciones de trabajo.
- Errores de administración aplicados a los aplicativos.
- Abuso de privilegios de acceso
- Desconocimiento de sus funciones y responsabilidades dentro de la empresa.
- Extorsión

Cualquiera de las infracciones o violaciones detalladas deben ser reportadas por medio del formulario de infracciones de políticas de seguridad[18]. Las mismas que deben ser reportadas al Jefe de Área, para que el mismo las remita al Jefe Nacional Administrativa.

Procedimientos Disciplinarios aplicables a Infracciones o Violaciones de Políticas de Seguridad
Todas las infracciones se verán afectadas por el siguiente flujo:

- Se realiza llamado de atención por escrito al infractor.
- Se detalla un memorándum donde se especifica el hecho realizado y la consecuencia del mismo. Las consecuencias son para la empresa y para el empleado tanto de tipo monetaria como para su hoja de vida.
- Cada infracción tiene una diferenciación en el procedimiento disciplinario, inscripta a continuación:

Infracción o Violación de Políticas de Seguridad	Procedimiento Disciplinario
Alteración, destrucción, divulgación y cambio de ubicación de información (Dentro y fuera de la compañía).	Llamado de atención en la hoja de vida. Capacitación acerca de activos de información y su protección.
Uso inapropiado de los diferentes recursos (Acceso no autorizado).	Capacitación acerca de los recursos de la empresa y su uso autorizado.
Usurpación de identidad	Llamado de atención grave en la hoja de vida. Reunión directa con el Gerente Regional y la Jefe Nacional Administrativa.
Manipulación de credenciales de acceso (Ingreso del trabajo)	Llamado de atención grave en la hoja de vida. Reunión directa con el Gerente Regional y la Jefe Nacional Administrativa.

[18] Revisar Anexo 15: Formulario de Infracción de Políticas de Seguridad

Manipulación de la configuración de los aplicativos y recursos de las estaciones de trabajo.	Capacitación acerca de recursos informáticos de la compañía, a cargo de delegado de Jefe de Área Sistemas.
Errores de administración aplicados al software informático.	Reunión con el Jefe de Área Sistemas. Revisión del Manual de Funciones y Responsabilidades del área Sistemas.
Abuso de privilegios de acceso	Llamado de atención en la hoja de vida. Capacitación acerca de recursos informáticos de la compañía, a cargo de delegado de Jefe de Área Sistemas.
Desconocimiento de sus funciones y responsabilidades dentro de la empresa.	Llamado de atención en la hoja de vida. Reunión con el Jefe de Área para revisión de Manual de Funciones y Responsabilidad del área al cual pertenezca el infractor.
Extorsión	Separación de la empresa.

Tabla 5. 1 Infracciones o Violaciones de Políticas de Seguridad

La aplicación de cualquier procedimiento disciplinario será supervisada por el encargado de la misma de mayor rango jerárquico y generara un formulario de seguimiento de aplicación de procedimientos disciplinarios[19]. Cada procedimiento disciplinario generara un archivo final que reflejara lo dispuesto, según la sanción. Toda la documentación que arroje cualquiera de los procedimientos disciplinarios será archivada en la Carpeta de Personal.

Detección de las Infracciones o Violaciones de Políticas de Seguridad:

Infracción o Violación de Políticas de Seguridad	Procedimiento de Detección
Alteración, destrucción, divulgación y cambio de ubicación de información (Dentro y fuera de la compañía).	Falta o modificación de la información, detectada mediante consulta de la misma. Divulgación escrita o verbal de información Conocimiento de información por personas externas a la empresa
Uso inapropiado de los diferentes recursos (Acceso no autorizado).	Observación visual Revisión de recursos mal utilizados

[19] Revisar Anexo 15: Formulario de Registro de Aplicación de Procedimientos Disciplinarios.

Usurpación de identidad	Doble inicio de sesión Manipulación de la configuración de usuario o de las opciones permitidas al mismo.
Manipulación de credenciales de acceso (Ingreso del trabajo)	Alteraciones en la credencial de acceso
Manipulación de la configuración de los aplicativos y recursos de las estaciones de trabajo.	Observación visual, incluye reubicación Comprobación de manipulación de aplicativo por otro usuario Inhabilitación del usuario por manipulación de usuario.
Errores de administración aplicados al software informático.	Fallas del aplicativo en el nivel de clientes Fallas en los privilegios de acceso (Desactivar acceso de páginas web para desarrollo de trabajo)
Abuso de privilegios de acceso	Observación visual Atraso de la productividad por uso inapropiado de los recursos informáticos
Desconocimiento de sus funciones y responsabilidades dentro de la empresa.	Mal desempeño de sus actividades Intermisión en las actividades de otro empleado Atraso de la productividad
Extorsión	Prueba escrita recibida por cualquier medio, que muestra la extorsión (Dentro o fuera de la empresa)

Tabla 5. 2 Detección de las Infracciones o Violaciones de Políticas de Seguridad

Aplicación de los Procedimientos Disciplinarios

Los Jefes de Área

- Detecta la infracción y envía por llamado de atención por escrito al infractor.
- Realiza memorándum donde se especifica el hecho realizado y la consecuencia del mismo.
- Envía los documentos a la Jefe Nacional Administrativa para realizar la aplicación de los procedimientos disciplinarios.
- Realiza la capacitación si el caso lo requiere.

La Jefe Nacional Administrativa

- Colabora con la definición de los procedimientos disciplinarios.
- Revisa la documentación enviada por cualquier Jefe de Área en caso de infracción o violación de políticas de seguridad.
- Aplica el procedimiento disciplinario según la infracción realizada.

- Reporta al Jefe Administrativo - Recursos Humanos, la documentación resultante de la aplicación del procedimiento disciplinario.

El Gerente

- Define los procedimientos disciplinarios en colaboración con la Jefe Nacional Administrativa.
- Colabora con la aplicación de los procedimientos disciplinarios dependiendo de la infracción.

Los empleados

- Conocen los procedimientos disciplinarios.
- Evitan infringir las políticas y procedimientos de seguridad de información.
- Acatan los procedimientos disciplinarios, según su infracción. Se acogen a las actividades a seguir.

Actualización de los Procedimientos Disciplinarios

Si se presentan infracciones o violaciones a políticas de seguridad que se consideran relevantes y que se realicen por primera vez, se debe adjuntar a los Tipos de Infracciones y Violaciones de Políticas de Seguridad.

Los Jefes de Área

- Redactan un informe, detallando la infracción, las consecuencias para el empleado y para la empresa y la forma como fue detectada. Dicho informe es remitido a la Jefe Nacional Administrativa.

La Jefe Nacional Administrativa

- Analiza el informe enviado por cualquiera de los Jefes de Área y determina el nivel de afectación de la infracción. Toda esta información la remite a la Gerencia para que apruebe la agregación.

- Si la infracción se determina importante, es incluida en los Tipos de Infracciones y Violaciones de Políticas de Seguridad.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones y Recomendaciones

La gestión de la seguridad de la información se realiza mediante un proceso sistemático, documentado y conocido por toda la organización. La utilización de un SGSI permite dotar a la entidad de las herramientas o mecanismos necesarios para poder afrontar los riesgos presentes en las empresas.

Una de las razones más importantes para implementar un SGSI es la de atenuar los riesgos propios de los activos de información de la empresa. Una acertada identificación de tales activos, su definición correcta del alcance y unas políticas de seguridad claras y completas, son determinantes para la correcta implantación del SGSI.

Un SGSI no se ajusta cada vez que se genera un incidente de seguridad, pues la labor de quienes tienen la función de gerencia de seguridad de la información en la empresa no debe ser únicamente la administración de los controles creados para cada situación de riesgo. Se debe actuar de manera que se anticipe a los hechos y para ello el SGSI debe estar en capacidad de ayudar a la alta gerencia en la definición de acciones que mitigan los riesgos sobre los activos más críticos sin tener que esperar que los eventos ocurran.

La implantación y operación de un SGSI ofrece ventajas para la empresa al disponer de una metodología dedicada a la seguridad de la información reconocida internacionalmente, contar con un proceso definido para evaluar, implementar, mantener y administrar la seguridad de la información, diferencia una empresa de otro con esto satisfacemos de una mejor manera los requerimientos de clientes, proveedores y organismos de control, formalizando las responsabilidades operativas y legales de los usuarios internos y externos de la Información y ayuda al cumplimiento de las disposiciones legales nacionales e internacionales.

ANEXOS

ANEXOS:

ANEXO 1: Definiciones y Términos

Secciones de control según ISO 27002
Política de Seguridad: Documento de política de seguridad y su gestión.
Aspectos Organizativos: Organización interna; organización externa.
Gestión de Activos: Responsabilidad sobre los activos; clasificación de la información.
Recursos Humanos: Anterior al empleo; durante el empleo; finalización o cambio de empleo.
Física y Ambiental: Áreas seguras; seguridad de los equipos.
Comunicaciones y Operaciones: Procedimientos y responsabilidades de operación; gestión de servicios de terceras partes; planificación y aceptación del sistema; protección contra software malicioso; backup; gestión de seguridad de redes; utilización de soportes de información; intercambio de información y software; servicios de comercio electrónico; monitorización.
Control de Accesos: Requisitos de negocio para el control de accesos; gestión de acceso de usuario; responsabilidades del usuario; control de acceso en red; control de acceso al sistema operativo; control de acceso a las aplicaciones e informaciones; informática y conexión móvil.
Adquisición: desarrollo y mantenimiento de sistemas: Requisitos de seguridad de los sistemas de información; procesamiento correcto en aplicaciones; controles criptográficos; seguridad de los ficheros del sistema; seguridad en los procesos de desarrollo y soporte; gestión de vulnerabilidades técnicas.
Gestión de incidentes: Comunicación de eventos y puntos débiles de seguridad de la información; gestión de incidentes y mejoras de seguridad de la información.
Gestión Continuidad de negocio: Aspectos de la seguridad de la información en la gestión de continuidad del negocio.
Cumplimiento legal: Con los requisitos legales; políticas de seguridad y estándares de conformidad y conformidad técnica; consideraciones sobre la auditoría de sistemas de información.
ISO: International Organization for Standardization, por sus siglas en ingles. Organización internacional para estandarización.
IEC: International Electrotecnical Commite, por sus siglas en ingles. Comisión electrotécnica internacional.

ANEXO 2: Descripción de cada puesto de trabajo

TÍTULO DEL PUESTO	DEPARTAMENTO	DESCRIPCIÓN DEL CARGO
Representante de la dirección	Gestión de Calidad	Responsable de promover el desarrollo, implantación y mantenimiento del Sistema de Gestión de Calidad que la empresa está tramitando.
Gerente	Dirección	El Gerente, es el responsable del manejo de la empresa y del cumplimiento de sus objetivos principales y particulares.
Jefe nacional de compensación y liquidación	Compensación y liquidación	Responsable de revisar, supervisar y controlar las negociaciones extrabursátiles y los procesos de compensación de Guayaquil y Quito, brindando apoyo en la información requerida por las casas de valores.
Jefe nacional de custodia y ejercicio de derecho	Custodia y ejercicio derecho	Responsable de la verificación, confirmación, seguridad y conservación de los valores recibidos en depósito, hasta su restitución o liquidación.
Jefe nacional de gestión de cobro y libro de acciones	Gestión de cobro y libro de acciones	Responsable de realizar la gestión de cobro ante los emisores o agentes de pago, y realizar el pago correspondiente a los inversionistas; registrar los movimientos en la cuenta del Emisor y dar constancia de los valores cancelados.
Jefe nacional de sistemas	Sistemas	Responsable de dirigir y planificar el desarrollo, implantación y mantenimiento de los sistemas tecnológicos de la organización.
Jefe nacional administrativa	Administrativo – recursos humanos	Administrar eficazmente el buen funcionamiento de la Institución y atender las necesidades de todo el personal con respecto a la relación laboral.
Asistente administrativa	Administrativo – recursos humanos	Asistir eficazmente en el buen funcionamiento de la Institución y atender las necesidades de todo el personal con respecto a la relación laboral.
Asistente de custodia y ejercicio de derecho	Custodia y ejercicio de derecho	El Asistente de Custodia y Ejercicio de Derecho es el recurso de apoyo para

		mantener los portafolios de los clientes al día.
Asistente de sistemas	Sistemas	Responsable de dar asistencia en la planificación y desarrollo de proyectos del área y ejecutar disposiciones tomadas por el jefe del departamento.
Jefe regional sierra de compensación y liquidación	Compensación y liquidación	Responsable de revisar, supervisar y controlar las negociaciones extrabursátiles y los procesos de compensación y liquidación en Quito, brindando apoyo en la información requerida por las casas de valores.
Jefe regional sierra de gestión de cobro y libro de acciones	Gestión de cobro y libro de acciones	Llevar el libro de acciones desmaterializadas de corporación Favorita.
Asistente de gestión de cobro y libro de acciones	Gestión de cobro y libro de acciones	Es el recurso de apoyo para mantener los portafolios de los clientes al día y verifica las transferencias realizadas.
Ayudante de administración	Administrativo / recursos humanos	Es un cargo de apoyo y soporte para el departamento de administración. Es responsable de mantener el orden y aseo de la cafetería a su cargo.
Desarrollador y técnico de soporte de sistemas	Sistemas	Responsable del desarrollo de los programas (Aplicaciones) que son parte de los proyectos informáticos y de cumplir con las tareas que correspondan a la asistencia técnica a usuarios encomendadas por el jefe o Asistente del Departamento de Sistemas.
Mensajero	Administrativo / recursos humanos	Responsable por la distribución y recolección de la correspondencia interna y/o externa de la compañía, desde o hacia ésta. Eventualmente ejecuta labores de apoyo administrativo requeridas.
Asesor legal	Legal	Organizar, controlar y ejecutar las actividades legales de la empresa dentro de un marco normativo y regulatorio, manteniendo informado a la Gerencia del cumplimiento de los objetivos fijados así como sus requerimientos.
Contadora	Contabilidad	Responsable por el control y supervisión de las operaciones y procedimientos contables de la compañía. Responde por la

		recopilación, análisis y registro contable, de acuerdo a las normas y procedimientos establecidos. Preparar estados financieros y otros informes.

Tabla Anexo. 1Descripción de cada puesto de trabajo

ANEXO 3: Perfil o Requisitos de los diferentes cargos

Cargo: Gerente
Sexo: Femenino o Masculino
Edad: Mínimo 35 años

Parámetros	Requisitos
Formación Académica	Título de Postgrado: MBA, MAE o similares
	Título Profesional de: Administración de Empresas o carreras afines certificado por el CONESUP
Experiencia Laboral	Entre 5 y 9 años de experiencia laboral en actividades gerenciales afines
Habilidades	Excelentes relaciones personales y facilidad para relacionarse efectivamente con los clientes
	Capacidad de planificación y trabajo bajo presión
	Buen nivel de expresión oral
	Liderazgo para conducir al personal a su cargo

Tabla Anexo. 2Perfil de Cargo Gerente

Cargo: Asesor Legal
Sexo: Femenino o Masculino
Edad: Mínimo 35 años

Parámetros	Requisitos
Formación Académica	Título profesional de Abogado certificado por el CONESUP Titulo profesional de Abogado certificado por el CONESUP
Experiencia Laboral	Entre 3 y 5 años de experiencia laboral en actividades similares o afines al cargo
Habilidades	Excelentes relaciones personales y facilidad para relacionarse
	Capacidad para trabajar bajo presión
	Buen nivel de expresión oral y extrovertido
	Capacidad para interactuar con grupos de trabajo
	Liderazgo para conducir al personal a su cargo

Tabla 7. 3Perfil de Cargo Asesor Legal

Cargo: Jefe Nacional Administrativo
Sexo: Femenino o Masculino
Edad: Mínimo 30 años

Parámetros	Requisitos
Formación Académica	Título Universitario
	Egresado de carreras afines
Experiencia Laboral	Entre 5 y 7 años de experiencia laboral en el cargo o en actividades afines
Habilidades	Excelentes relaciones personales y facilidad para relacionarse efectivamente con los clientes
	Capacidad para trabajar bajo presión
	Buen nivel de expresión oral
	Capacidad para interactuar con grupos de trabajo
	Liderazgo para conducir al personal a su cargo
	Excelente presentación personal

Tabla 7. 4 Perfil de Cargo Jefe Nacional Administrativo

Cargo: Asistente Administrativo
Sexo: Femenino o Masculino
Edad: Mínimo 19 años

Parámetros	Requisitos
Formación Académica	Egresado universitario en áreas de competencia
	Estudiante universitario en áreas de competencia
	Título de bachiller en cualquier especialización
Experiencia Laboral	Menos de 2 años en puestos similares o afines
Habilidades	Para relacionarse efectivamente con clientes
	Capacidad para organizar y coordinar tareas administrativas
	Para integrar e interactuar en grupos de trabajo
	Capacidad para trabajar bajo presión
	Excelente presentación personal

Tabla 7. 5 Perfil de Cargo Asistente Administrativo

Cargo: Ayudante de Administración
Sexo: Femenino
Edad: Mínimo 20 años

Parámetros	Requisitos
Formación Académica	Bachiller en cualquier especialización
Experiencia Laboral	Mínimo 1año de experiencia en cargos similares o afines
Habilidades	Capacidad para interpretar y ejecutar directrices
	Iniciativa para el cumplimiento de las tareas encomendadas
	Capacidad para trabajar bajo presión
	Buena presentación personal
	Para relacionarse efectivamente

Tabla 7. 6 Perfil de Cargo Ayudante de Administración

Cargo: Mensajero
Sexo: Masculino
Edad: Mínimo 20 años

Parámetros	Requisitos
Formación Académica	Estudiante en carreras superiores
	Bachiller en cualquier especialización
Experiencia Laboral	Mínimo 1año de experiencia en cargos similares o afines
Habilidades	Capacidad para interpretar y ejecutar directrices
	Iniciativa para el cumplimiento de las tareas encomendadas
	Capacidad para trabajar bajo presión
	Buena presentación personal
	Para relacionarse efectivamente

Tabla 7. 7 Perfil de Cargo Mensajero

Cargo: Representante de la Dirección
Sexo: Femenino o Masculino
Edad: Mínimo 24 años

Parámetros	Requisitos
Formación Académica	Título en carreras superiores
	Egresado en carreras superiores
	Estudiante en carreras superiores
Experiencia Laboral	Mínimo 5 años de experiencia laboral en actividades similares o afines al cargo
	Entre 3 y 5 años de experiencia laboral en actividades similares o afines al cargo
Habilidades	Excelentes relaciones personales y facilidad para relacionarse
	Capacidad de planificación
	Capacidad para trabajar bajo presión
	Buen nivel de expresión oral
	Capacidad para interactuar con grupos de trabajo

Tabla 7. 8 Perfil de Cargo Representante de la Dirección

Cargo: Contador
Sexo: Femenino o Masculino
Edad: Mínimo 35 años

Parámetros	Requisitos
Formación Académica	Título Universitario en contabilidad, contaduría pública o carreras afines
	Egresado Universitario en áreas de competencia
Experiencia Laboral	Entre 3 y 5 años de experiencia laboral en actividades similares o afines al cargo
Habilidades	Excelentes relaciones personales y facilidad para relacionarse
	Capacidad para definir parámetros y objetivos deseados
	Capacidad para trabajar bajo presión
	Buen nivel de expresión oral
	Capacidad para interactuar con grupos de trabajo

Tabla 7. 9 Perfil de Cargo Contador

Cargo: Jefe de Gestión de Cobro / Jefe Regional Sierra de Gestión de Cobro y Libro de Acciones
Sexo: Femenino o Masculino
Edad: Mínimo 30 años

Parámetros	Requisitos
Formación Académica	Título Universitario en áreas de competencia
	Egresado Universitario en áreas de competencia
Experiencia Laboral	Entre 3 y 5 años de experiencia en cargos afines o similares
Habilidades	Para relacionarse efectivamente con clientes
	Capacidad para definir parámetros y objetivos deseados
	Liderazgo para conducir al personal a su cargo
	Para integrar e interactuar en grupos de trabajo
	Capacidad para trabajar bajo presión
	Buen nivel de expresión oral

Tabla 7. 10 Perfil de Cargo Jefe de Gestión de Cobro / Jefe Regional Sierra de Gestión de Cobro y Libro de Acciones

Cargo: Asistente de Gestión de Cobro y Libro de Acciones
Sexo: Femenino o Masculino
Edad: Mínimo 20 años

Parámetros	Requisitos
Formación Académica	Título Universitario en áreas de competencia
	Egresado universitario en áreas de competencia
Experiencia Laboral	Más de 3 años en puestos similares o afines
Habilidades	Para relacionarse efectivamente con clientes
	Capacidad para organizar y coordinar tareas administrativas
	Para integrar e interactuar en grupos de trabajo
	Capacidad para trabajar bajo presión
	Excelente presentación personal

Tabla 7. 11 Perfil de Cargo Asistente de Gestión de Cobro y Libro de Acciones

Cargo: Jefe Nacional de Custodia y Ejercicio de Derecho
Sexo: Femenino o Masculino
Edad: Mínimo 30 años

Parámetros	Requisitos
Formación Académica	Título Universitario en áreas de competencia
	Egresado Universitario en áreas de competencia
Experiencia Laboral	Entre 3 y 5 años de experiencia en cargos afines o similares
Habilidades	Para relacionarse efectivamente con clientes
	Capacidad para definir parámetros y objetivos deseados
	Liderazgo para conducir al personal a su cargo
	Para integrar e interactuar en grupos de trabajo
	Capacidad para trabajar bajo presión
	Buen nivel de expresión oral

Tabla 7. 12 Perfil de Cargo Jefe Nacional de Custodia y Ejercicio de Derecho

Cargo: Asistente de Custodia y Ejercicio de Derecho
Sexo: Femenino o Masculino
Edad: Mínimo 20 años

Parámetros	Requisitos
Formación Académica	Egresado universitario en áreas de competencia
	Estudiante universitario en áreas de competencia
Experiencia Laboral	Más de 3 años en puestos similares o afines
Habilidades	Para relacionarse efectivamente con clientes
	Capacidad para organizar y coordinar tareas administrativas
	Para integrar e interactuar en grupos de trabajo
	Capacidad para trabajar bajo presión
	Excelente presentación personal

Tabla 7. 13 Perfil de Cargo Asistente de Custodia y Ejercicio de Derecho

Cargo: Jefe Nacional de Compensación y Liquidación
Sexo: Femenino o Masculino
Edad: Mínimo 30 años

Parámetros	Requisitos
Formación Académica	Título Universitario en áreas de competencia
	Egresado Universitario en áreas de competencia
Experiencia Laboral	Entre 3 y 5 años de experiencia laboral en actividades similares o afines al cargo
Habilidades	Excelentes relaciones personales y facilidad para relacionarse efectivamente con los clientes
	Capacidad para definir parámetros y objetivos deseados
	Capacidad para trabajar bajo presión
	Buen nivel de expresión oral
	Capacidad para interactuar con grupos de trabajo
	Liderazgo para conducir al personal a su cargo

Tabla 7. 14 Perfil de Cargo Jefe Nacional de Compensación Y Liquidación

Cargo: Asistente de Compensación y Liquidación
Sexo: Femenino o Masculino
Edad: Mínimo 20 años

Parámetros	Requisitos
Formación Académica	Egresado universitario en áreas de competencia
	Estudiante universitario en áreas de competencia
Experiencia Laboral	Menos de 2 años de experiencia en cargos similares o afines
Habilidades	Capacidad para ejecutar directrices
	Buen trato con el cliente
	Iniciativa para el cumplimiento de las tareas encomendadas
	Capacidad para trabajar bajo presión
	Buena presentación personal

Tabla 7. 15 Perfil de Cargo Asistente de Compensación y Liquidación

Cargo: Jefe de Sistemas
Sexo: Femenino o Masculino
Edad: Mínimo 30 años

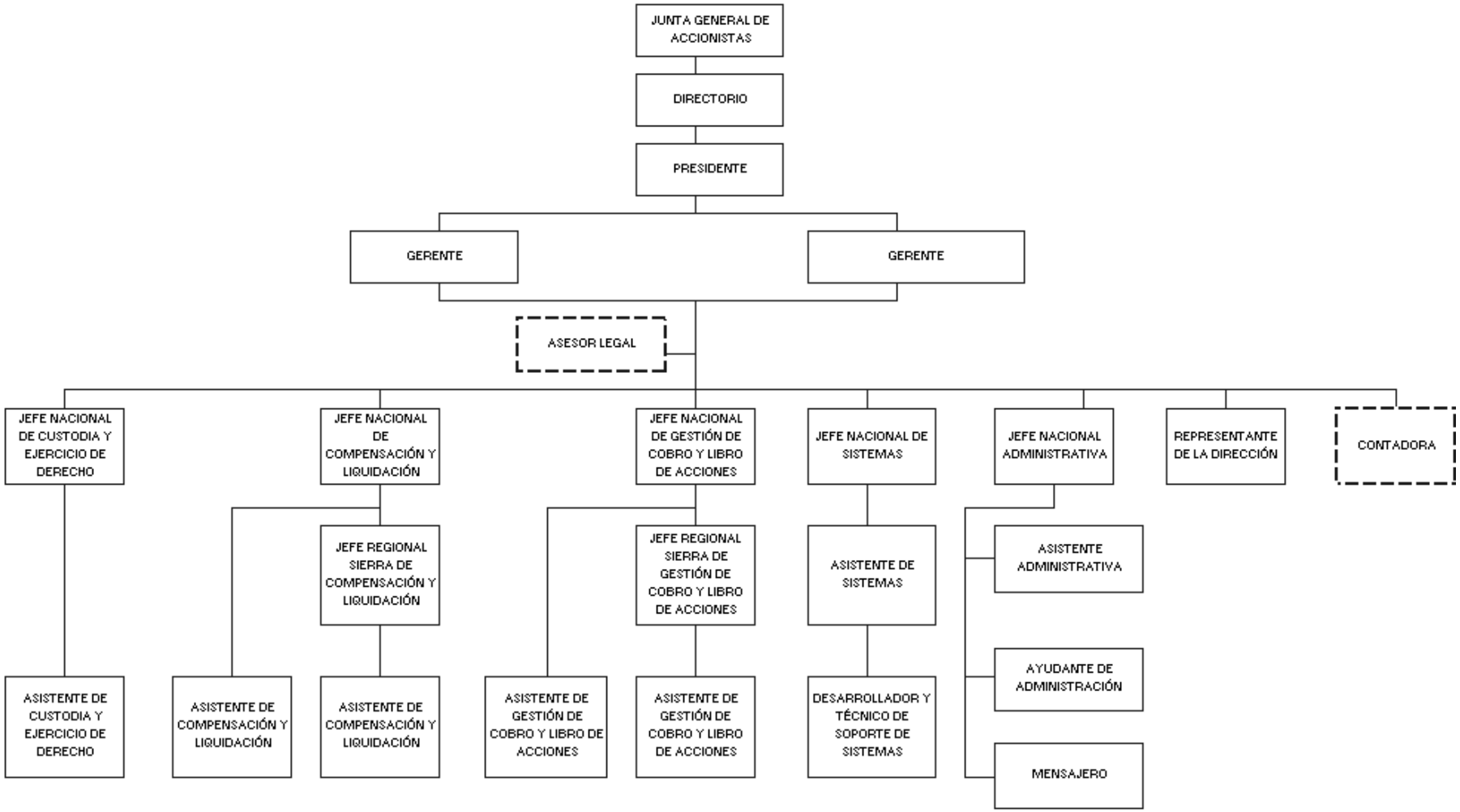
Parámetros	Requisitos
Formación Académica	Título profesional de Ingeniero en Sistemas
	Titulo en carreras afines acreditado por el CONESUP
Experiencia Laboral	Más de 3 años de experiencia en el cargo o en posiciones similares
Habilidades	Excelentes relaciones personales y facilidad para relacionarse
	Capacidad de planificación
	Capacidad para trabajar bajo presión
	Liderazgo para conducir al personal a su cargo

Tabla 7. 16 Perfil de Cargo Jefe de Sistemas

Cargo: Asistente de Sistemas / Desarrollador
Sexo: Femenino o Masculino
Edad: Mínimo 20 años

Parámetros	Requisitos
Formación Académica	Estudiante en la carrera de Ingeniería en Sistemas
	Estudiante universitario en carreras afines acreditado por el CONESUP
Experiencia Laboral	Más de 2 años de experiencia en el cargo o en posiciones similares
Habilidades	Excelentes relaciones personales y facilidad para relacionarse
	Capacidad para ejecutar directrices
	Capacidad para trabajar bajo presión
	Iniciativa para el cumplimiento de tareas encomendadas

Tabla 7. 17 Perfil de Cargo Asistente de Sistemas / Desarrollador



ANEXO 4: Organigrama de la empresa

ANEXO 5: Escala de Valoración de los Activos

5.1 Escala de Valoración de Dimensiones:

Descripción	Valoración
Alta	5
Medianamente Alta	4
Mediana	3
Baja	2
Muy Baja	1

Tabla 7. 18 Escala de Valoración de Dimensiones

5.2 Escala de Valoración de Frecuencia:

Descripción	Valoración
Altamente Frecuente	5
Frecuente	4
Medianamente Frecuente	3
Poco Frecuente	2
Muy Poco Frecuente	1

Tabla 7. 19 Escala de Valoración de Frecuencia

5.3 Escala de Valoración de Impacto:

Descripción	Valoración
Alto	5
Medianamente Alto	4
Mediano	3
Bajo	2
Muy Bajo	1

Tabla 7. 20 Escala de Valoración de Impacto

Firma del Encuestado *Firma de Revisión*

echa de Revisión: _____

ANEXO 6:

Formulario de Aplicabilidad de las Políticas de Seguridad

FORMULARIO DE APLICABILIDAD
DE POLÍTICAS DE SEGURIDAD

NOMBRE DEL ENCUESTADO: _____
FECHA : _____
CARGO : _____
ÁREA DE TRABAJO : _____

Instrucciones: Debe responder las preguntas de manera honesta y responsable. Sus respuestas deben ser claras y concisas. Por favor, entregue el formulario sin tachones, ni arrugas.

1. *¿Conoce las políticas de Seguridad de Información que se aplican en su área de trabajo?*

Respuesta: _____

2. *¿Ha sido informado a tiempo de las políticas de seguridad de información?*

Respuesta: _____

3. ¿Conoce las infracciones o violaciones de las políticas de Seguridad de Información?
Respuesta: _____

4. ¿Ha sido informado a tiempo de los procedimientos disciplinarios?
Respuesta: _____

5. ¿Cuán dañino considera que puede ser la alteración o divulgación de la información?
Respuesta: _____

6. ¿Cuáles es su horario de acceso al servicio de Internet?
Respuesta: _____

7. ¿Cuáles son seguridades de la credencial de acceso del personal?
Respuesta: _____

8. ¿Cuál es su principal función dentro de la empresa?
Respuesta: _____

9. ¿Cuál es la actividad que más repite durante su jornada de trabajo?
Respuesta: _____

10. ¿Considera relevante aplicar políticas de seguridad de información en la empresa?
Respuesta: _____

Los Formularios de Aplicabilidad de Seguridad de la Información pueden variar dependiendo de área al cual sea aplicado. Además, los formularios deben ser actualizados al inicio de cada año. Esta responsabilidad es del Gerente y la Jefe Nacional Administrativa.

ANEXO 7: Registro de Inconformidades

REGISTRO DE INCONFOMIDADES
EN EL FORMULARIO DE APLICABILIDAD
DE POLÍTICAS DE SEGURIDAD

FECHA: _____

EMPLEADO	ÁREA DE TRABAJO	OBSERVACIÓN	ACCIÓN
(Nombre de Empleado de la observación)	(Área de Trabajo del Empleado)	(Observación reflejada en el formulario aplicado)	(Capacitación o Reunión de Revisión de Políticas de Seguridad)

_____
Firma de Elaboración

Fecha de Revisión (Gerencia): _____

En el registro de inconformidades se guarda algunas observaciones y acciones a tomar, dependiendo de los reflejados en los formularios. Debe ser enviado al Gerente por la Jefe Nacional Administrativa.

ANEXO 8: Plan de Verificación de Aplicabilidad de Seguridades

PLAN DE VERIFICACIÓN DE APLICABILIDAD DE POLÍTICAS DE SEGURIDAD

El Plan de Verificación de Aplicabilidad de Políticas de Seguridad es elaborado por la Jefe Nacional Administrativa y aprobado por el Gerente. Debe contener las actividades de verificación planeadas al principio del año. Su actualización se podría dar dependiendo de las necesidades de verificación relevantes.

FECHA DE PLANIFICACIÓN: _____
PERÍODO : _____

FECHA DE APLICACIÓN	ÁREA DE TRABAJO	CAUSA DE LA APLICACIÓN	FORMULARIO A APLICAR	LUGAR DE APLICACIÓN	SUPERVISOR	JUSTIFICACIÓN DE INCUMPLIMIENTO	OBSERVACIONES
(Fecha planeada para aplicación de verificación de aplicabilidad)	(Área planeada para la fecha)	(Razón de la aplicación planeada)	(Formulario a Implementar)	(Lugar de aplicación de la verificación)	(Nombre del Jefe que supervisara la aplicación de la verificación)	(Razones de incumplimiento de la verificación planificada)	(Posibles notas agregadas a la verificación planeada)

_____ _____
Firma de Elaboración *Firma de Aprobación*

Fecha de Aprobación: _____

ANEXO 9: Boletín de información: Plan de Verificación de Aplicabilidad

ANEXO 10: Formulario de Control de Asistencia de Verificación de Aplicabilidad

REGISTRO DE ASISTENCIA DE
VERIFICACIÓN DE APLICABILIDAD DE POLÍTICAS DE SEGURIDAD

FECHA DE VERIFICACIÓN: _____
FORMULARIO APLICADO: _____
LUGAR DE APLICACIÓN : _____
SUPERVISOR : _____

EMPLEADO	HORA DE ENTRADA	FIRMA	HORA DE SALIDA	FIRMA
(Nombre del empleado que realiza el formulario de verificación)	(Hora que ingresa a la verificación)	(Firma de constancia de la entrada del empleado)	(Hora que egresa a la verificación)	(Firma de constancia de la salida del empleado)

_____ _____
Firma de Supervisión *Firma de Revisión*

Fecha de Revisión: _____

ANEXO 11: Plan de Capacitación: Seguridad de la Información

PLAN DE CAPACITACIÓN DE SEGURIDAD DE LA INFORMACIÓN

FECHA DE PLANIFICACIÓN: _____
PERÍODO : _____

FECHA DE APLICACIÓN	ÁREA DE TRABAJO	CAUSA DE LA CAPACITACIÓN	TEMA A TRANSMITIR	NÚMERO DE HORAS	LUGAR DE LA CAPACITACIÓN	CAPACITADOR	JUSTIFICACIÓN DE INCUMPLIMIENTO	OBSERVACIONES
(Fecha planeada para la capacitación)	(Área planeada para la fecha)	(Razón de la capacitación planeada)	(Tema de la capacitación)	(Total de horas de duración de la capacitación planeada)	(Lugar de la capacitación)	(Nombre del Jefe que supervisara la aplicación de la verificación)	(Razones de incumplimiento de la verificación planificada)	(Posibles notas agregadas a la verificación planeada)

_____ _____
Firma de Elaboración *Firma de Aprobación*

Fecha de Aprobación: _____

ANEXO 12: Carta de convocatoria a empleados.

FECHA DE CREACIÓN

Nombre del Empleado
Área de Trabajo

De mis consideraciones:

Por medio de la presente se le convoca a la capacitación <<NOMBRE DE LA CAPACITACIÓN>>, dictada por <<NOMBRE DEL CAPACITADOR>>, a efectuarse el día<<FECHA DE LA CAPACITACIÓN>>, a las <<HORA DE LA CAPACITACIÓN>> en las instalaciones de <<LUGAR DE LA CAPACITACIÓN>>, donde se reforzara su entrenamiento con respecto a las políticas y procedimientos de seguridad de la información aplicados en la empresa.

Le recordamos que su presencia es obligatoria.

NOMBRE DE LA JEFE NACIONAL ADMINISTRATIVA

La carta puede ser editada para agregar más detalles, dependiendo de la convocatoria a realizar. Además, podría cambiar el pie de firma, según las disposiciones gerenciales.

ANEXO 13: Formulario de Control de Asistencia a Capacitación

REGISTRO DE ASISTENCIA DE
CAPACITACIÓN DE SEGURIDAD DE INFORMACIÓN

FECHA DE CAPACITACIÓN: _____
LUGAR DE CAPACITACIÓN: _____
CAPACITADOR : _____
TEMA : _____

EMPLEADO	HORA DE ENTRADA	FIRMA	HORA DE SALIDA	FIRMA
(Nombre del empleado que se está capacitando)	(Hora que ingresa a la capacitación)	(Firma de constancia de la entrada del empleado)	(Hora que egresa a la capacitación)	(Firma de constancia de la salida del empleado)

_____ _____
Firma de Supervisión *Firma de Revisión*

Fecha de Revisión: _____

ANEXO 14: Formulario de Infracción de Políticas de Seguridad.

FORMULARIO DE REGISTRO
DE INFRACCIONES O VIOLACIONES DE POLÍTICAS DE SEGURIDAD

ELABORADO POR: _____

FECHA	EMPLEADO	ÁREA DE TRABAJO	INFRACCIÓN	SITUACIÓN	ACCIÓN
(Fecha de realiza la infracción)	(Nombre de Empleado que comete la infracción)	(Área de Trabajo del Empleado)	(Infracción incurrida)	(Detalle de la situación de la infracción)	(Procedimiento Disciplinario a aplicar por motivo de la infracción)

Firma de Elaboración

Fecha de Revisión (Gerencia):

En el Registro de Infracciones o Violaciones de Políticas de Seguridad se guarda los detalles correspondientes a situaciones que quebrantan los procedimientos de seguridad de información que se encuentran implementados en la empresa y los procedimientos disciplinarios a aplicar por los mismos. Debe ser enviado al Gerente por la Jefe Nacional Administrativa.

ANEXO 15: Seguimiento de la Aplicación de los Procedimientos Disciplinarios

FORMULARIO DE SEGUIMIENTO
DE PROCEDIMIENTOS DISCIPLINARIOS

SUPERVISADO POR: _____

FECHA	EMPLEADO	ÁREA DE TRABAJO	GESTOR	ACCIÓN DE SEGUIMIENTO
(Fecha de seguimiento)	(Nombre de Empleado que comete la infracción)	(Área de Trabajo del Empleado)	(Persona que aplica el procedimiento disciplinario)	(Situaciones que permiten aplicar el procedimiento disciplinario)

_____
Firma de Elaboración

Fecha de Revisión (Gerencia): _____

En caso de que la infracción incurrida sea Extorsión o alguna otra que necesite separación del empleo, también debe registrarse en el formulario de seguimiento.

Documentación Privada de la empresa ACB INGENIERIA LTDA