ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

ESCUELA DE DISEÑO Y COMUNICACIÓN VISUAL

PROYECTO DE GRADUACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

ANALISTA DE SISTEMAS

TEMA:

"IMPLANTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICADA AL DOMINIO GESTIÓN DE ACTIVOS PARA LA EMPRESA PLÁSTICOS INTERNACIONALES PLASINCA C.A."

AUTORES:

ALEJANDRA EUGENIO RIVAS
MIGUEL PARRALES ESPINOZA
PAÚL SABANDO SUDARIO

DIRECTOR:

MBA. VÍCTOR MUÑOZ CHACHAPOLLA

AÑO
2011

AGRADECIMIENTO

A Dios, a nuestros padres por todo su apoyo incondicional y confianza, y a todas las personas que nos ayudaron a culminar nuestra carrera.

A nuestro Director de Tesis por su gran ayuda y colaboración.

DEDICATORIA

A nuestras familias y todos nuestros amigos quienes siempre de alguna manera nos ayudaron y apoyaron incondicionalmente.

DECLARACIÓN EXPRESA

La responsabilidad del contenido de este Trabajo Final de Graduación, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

(Reglamento de Graduación de Pregrado de la ESPOL).

FIRMA DEL DIRECTOR DEL PROYECTO Y DE LOS MIEMBROS DEL TRIBUNAL

_____

Mba. Víctor Muñoz Chachapolla

Director del Proyecto

_____

Delegado

FIRMAS DE LOS AUTORES DEL PROYECTO DE GRADUACIÓN

_____

Alejandra Eugenio Rivas

_____

Miguel Parrales Espinoza

_____

Paúl Sabando Sudario

RESUMEN

La información es un activo vital para la continuidad y el éxito en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan, por lo tanto este documento propone implementar un Sistema de Gestión de Seguridad de información (SGSI), aplicado al dominio Gestión de Activos. Basado en las normas ISO 27000, ISO 27001 e ISO 27002, las cuales proporcionan medidas de apoyo necesarias para proteger y mantener segura la información.

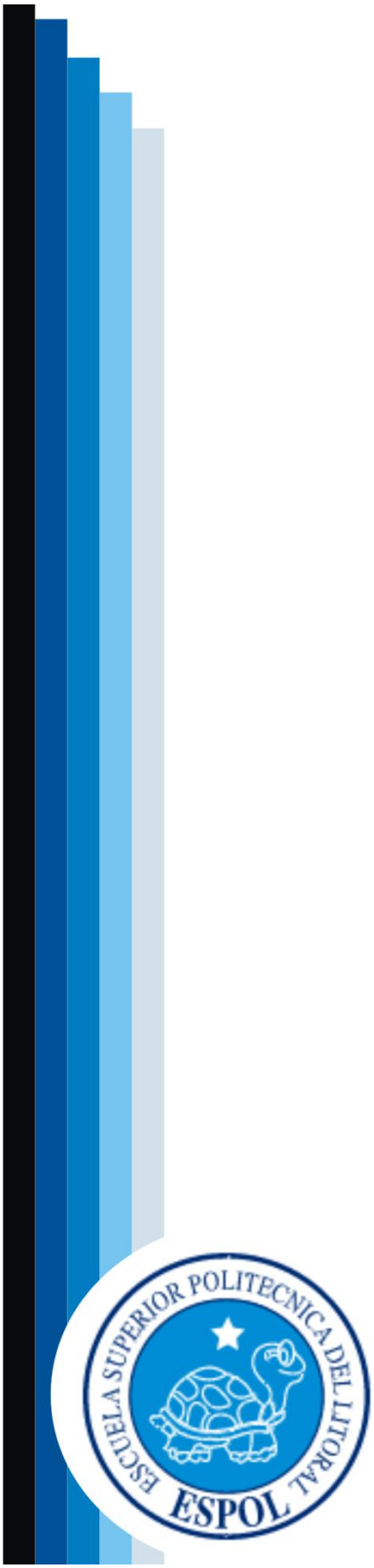
Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

Permitiendo a la organización, identificar los riesgos en el entorno de trabajo, ya sean existentes o latentes y determina la vulnerabilidad a la que están expuestos; recomendando las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir y controlar los riesgos identificados y así reducir al mínimo sus perjuicios.

ÍNDICE GENERAL

ÍNDICE DE FIGURA

ÍNDICE DE TABLAS



CAPÍTULO I
INTRODUCCIÓN

I. INTRODUCCIÓN

I.1 DEFINICIÓN

Plásticos Internacionales Plasinca C.A. es una empresa dedicada a la fabricación de empaques flexibles para el sector Agro Exportador y de Consumo. La planta industrial y oficinas se encuentran ubicadas en el Km. 10 ½ de la vía a Daule, Lotización Expogranos.

Figura - 1 Logo de la empresa

I.2 SITUACIÓN ACTUAL

En los actuales momentos cuenta con dos sistemas informáticos: uno de producción, que se encarga de llevar el manejo de la fabricación de productos y otro para la administración llamado Bi-moneda, que se encarga de la contabilidad. Estos sistemas informáticos generan una gran cantidad de información, la cual se deben mantener segura tomando medidas o políticas de seguridad para salvaguardar su información.

La empresa no cuenta con un Sistema de Gestión de Seguridad de la Información, por lo tanto están expuestos a pérdidas de activo muy valiosos, la cual perjudicaría funcionamiento de las actividades que realizan. A continuación detallaremos los principales inconvenientes que presenta la empresa:

- La empresa no cuenta con un inventario actualizado.
- Las laptops no están apropiadamente aseguradas a algo rígido.
- Solo existe un encargado en el Área de Sistemas.
- Hay equipos que no cuentan con un debido regulador de energía.
- Los computadores no tienen establecidos responsables.
- Algunos computadores no tienen la climatización necesaria.

I.3 ESTRUCTURA ORGANIZACIONAL

I.3.1 *MISIÓN*

Proveer a sus clientes productos y servicios que excedan sus expectativas, a un costo competitivo en el mercado, de tal forma que represente un ahorro en materia económica y una ventaja en términos de calidad, logrando satisfacer sus necesidades establecidas.

I.3.2 *VISIÓN*

Ser reconocida como una empresa Líder en el mercado de los productos de su género a nivel nacional y asegurar una competitividad sostenible y rentable permanentemente.

I.3.3 *POLÍTICAS DE CALIDAD*

Está orientada a implementar y mantener la mejora continua de los procesos del sistema de gestión de calidad y de su talento humano con lo cual garantizan la completa satisfacción del cliente interno y externo.

I.3.4 *POLÍTICAS DE SEGURIDAD*

Plásticos Internacionales C.A. está enfocada a la producción de material de empaque primario y secundario seguros y de calidad, cumpliendo con los requisitos de sus clientes, buscando su satisfacción mediante el aumento del desempeño de la seguridad alimentaria, a través de la aplicación de programas de mejora continua para prevenir, reducir y/o eliminar los riesgos, peligros, aspectos e impactos asociados a la seguridad alimentaria y el ambiente.

I.4 DIAGRAMA DE PLANTA

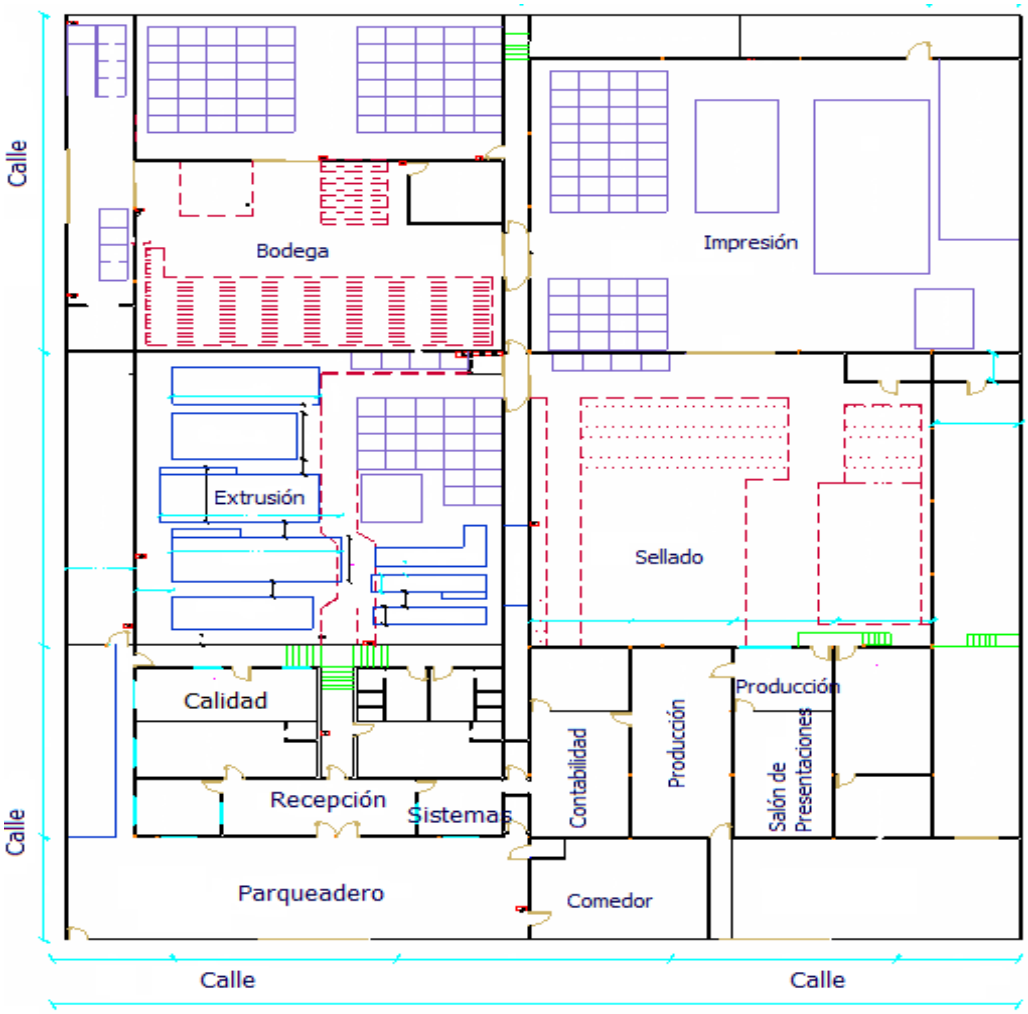


Figura - 2 Estructura de la empresa

I.5 FUNCIONAMIENTO POR ÁREA

Contabilidad	Es el encargado de realizar los Balances Generales, Control de Impuestos, Administración de Finanzas y acuerdos con los bancos.
Recepción	Hacen parte de la facturación y llevan el control de las ventas.
Producción	Realiza las órdenes de pedido, programa órdenes para el área de planta, validación de reportes y despachos.
Recursos Humanos	Inspección y monitoreo de los empleados, con la utilización de nóminas, fichas empleados, etc.
Sub-Gerencia	Lleva el control de la producción y de las ventas, también realiza funciones de ventas.
Extrusión	Encargado de la elaboración de reportes y de salvaguardar las mezclas para la fabricación de los productos.
Sellado	Se centra en la elaboración de fundas e ingresos a producción.
Impresión	Elaboración de reportes de la fabricación de royos impresos, laminados e ingresos a producción.
Calidad	Verifica que los productos lleguen en condiciones adecuadas a los clientes, también controla la manufactura de las aéreas anteriores y además el seguimiento de las devoluciones.
Bodega	Control de las existencias, seguimientos de las transferencias y verifica que los despachos lleguen al cliente de manera correcta.

Tabla 1 - Funcionamiento por Área

I.6 ORGANIGRAMA

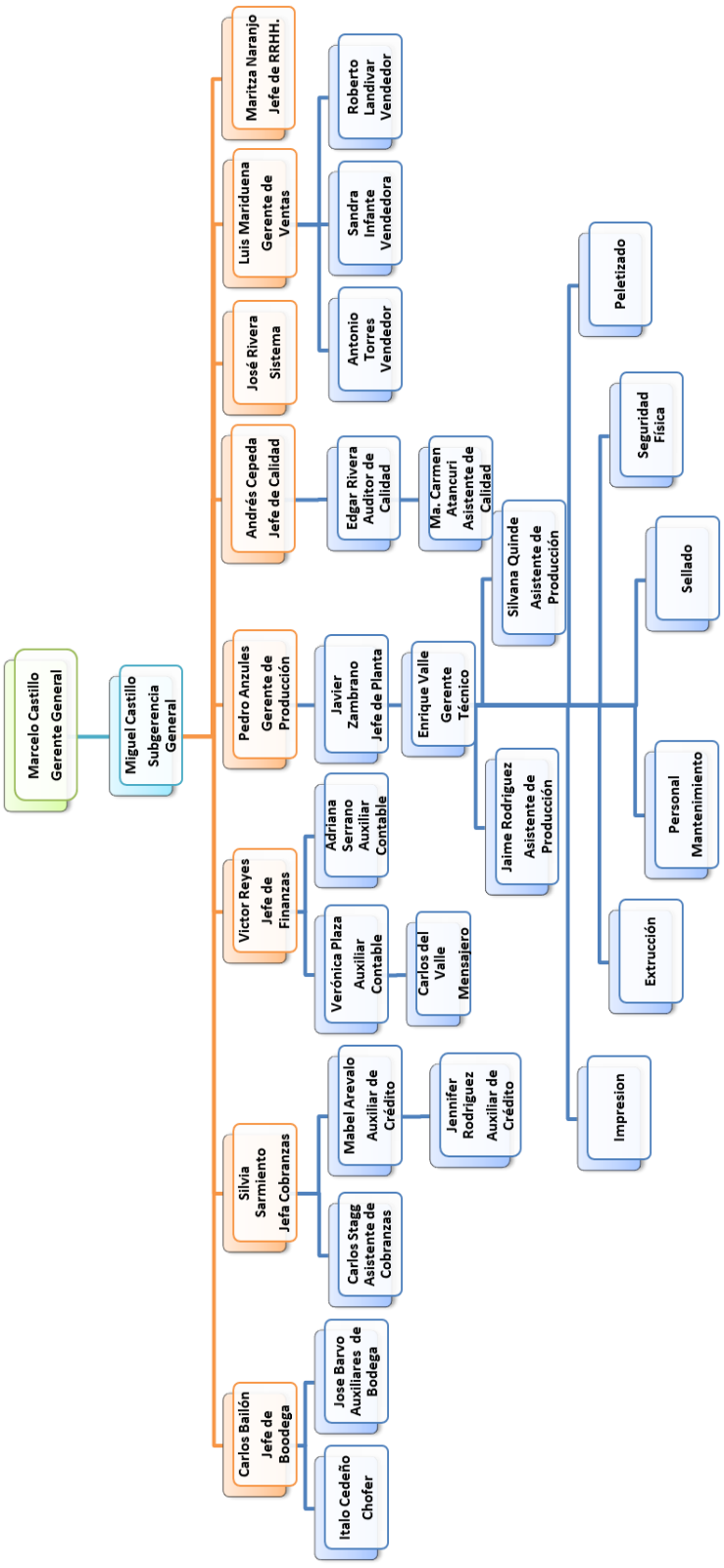


Figura - 3 Organigrama de la empresa

CAPÍTULO II

PLANEACIÓN DEL SGSI

II. PLANEACIÓN DEL SGSI

II.1 METODOLOGÍA DE EVALUACIÓN DE RIESGOS

En este caso específico usaremos el método de investigación de riesgos denominado Magerit, la cual nos recomendará las medidas apropiadas para controlar los activos.

La metodología Magerit nos muestra el grado de protección que tienen los activos con respecto al ambiente en que se encuentran y cómo interactúan con este, con el cual se podrá evaluar y posteriormente determinar la vulnerabilidad de estos equipos. Además de la implantación de controles para mejorar la manipulación y en lo posible tratar de disminuir la ocurrencia de los factores maliciosos, los cuales se podrían transformar en un impacto desfavorable para la organización.

Esta técnica nos proveerá la mejor funcionalidad, adecuada para reconocer las dependencias entre los activos más importantes por medio de un análisis algorítmico y un método que implica el reconocimiento de los riesgos y su valoración, para llegar a un nivel tolerable de los mismos. Con un esquema que nos ayudará a concienciar a los responsables de los activos de la existencia de los riesgos a la cual están expuestos.

Permite a la organización, identificar los riesgos en el entorno de trabajo, ya sean existentes o latentes y determina la vulnerabilidad a la que están expuestos; recomienda las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, y controlar los riesgos identificados y así reducir al mínimo sus perjuicios. Está compuesta de cuatro etapas, que nos aclara la forma de trabajar en este ámbito, que son:

- La Planificación se considera como el comienzo del proyecto y es donde se define lo que se va a cumplir.
- En el análisis de riesgos, se identifican y se cuantifica los activos, obteniendo una estimación deseable que se pueda controlar.
- La Gestión de riesgos identifica las funciones y servicios de salvaguardas que sirven para reducir el riesgo e implantar restricciones para el uso de los activos.
- Seleccionar las salvaguardas que incluyen el plan de implantación y los procedimientos de seguimiento, y se obtienen los resultados finales a diversos niveles.

II.2 IDENTIFICACIÓN Y VALORACIÓN DE ACTIVOS

II.2.1 *IDENTIFICACIÓN DE ACTIVOS*

Para la identificación de los activos se utilizaron los datos proporcionados por el Administrador de Sistemas, correspondientes al Inventario. Los activos de la empresa Plásticos Internacionales C.A. son:

NO.	ACTIVO	USUARIO	FUNCIÓN
1	WRKS-REC-001	Jennifer Rodríguez	▸ Elabora pedidos. ▸ Valida reportes.
2	WRKS-REC-002	Mabel Arévalo	▸ Control de despachos. ▸ Control de órdenes de Pedido. ▸ Cálculos de precio de pedido.
3	WRKS-PRE-003	No asignado	▸ Exposiciones de charlas educativas
4	WRKS-RRHH-004	Maritza Naranjo	▸ Contratación de Personal.

5	WRKS-CON-005	Víctor Reyes	▸ Elaboración de cuadros de amortizaciones y depreciaciones. ▸ Flujos de caja. ▸ Cuadro de obligaciones bancarias. ▸ Control de las importaciones de materia prima. ▸ Pago de Impuestos.
6	WRKS-CON-006	Verónica Plaza	▸ Elaboración de cuadros de importaciones. ▸ Elaboración de formularios de transferencia. ▸ Administrar la contabilidad.
7	WRKS-CON-007	Adriana Serrano	▸ Administrar los movimientos bancarios. ▸ Girar cheques. ▸ Proveeduría.
8	WRKS-PRO-008	Silvia Sarmiento	▸ Realizar liquidaciones. ▸ Inventario de materia prima.
9	WRKS-PRO-009	Carlos Stagg	▸ Elaborar cotizaciones. ▸ Elaborar reporte de ventas. ▸ Cobranzas.
10	WRKS-PRO-010	Pedro Azules	▸ Realizar compras externas de materia prima. ▸ Realizar órdenes de mantenimiento de maquinaria. ▸ Administrar el proceso de producción.
11	WRKS-PRO-011	Jaime Rodríguez	▸ Validar Reportes.
12	WRKS-PRO-012	Luis Valle	▸ Programar tareas de producción. ▸ Elaboración de cuadros de costos.
13	WRKS-PRO-024	Javier Zambrano	▸ Realizar órdenes de producción.

			▸ Realizar órdenes de extrusión. ▸ Realizar órdenes de sellado.
14	WRKS-PRO-013	Silvana Quinde	▸ Realizar fórmulas de producción. ▸ Control de estado de maquinarias.
15	WRKS-SEL-014	Víctor Cevallos	▸ Administrar el proceso de sellado.
16	WRKS-IMP-015	Enrique Valle	▸ Administrar etiquetado de productos terminados.
17	WRKS-CAL-017	María del Carmen	▸ Aprobar productos terminados.
18	WRKS-EXT-016	No asignado	▸ Administrar el proceso de extrusión.
19	WRKS-CAL-018	Andrés Cepeda	▸ Realizar proceso de calidad.
20	WRKS-BOD-019	Carlos Bailón	▸ Realizar cuadros de despachos.
21	WRKS-BOD-020	José Bravo	▸ Realizar cuadros de inventario de productos terminados.
22	WRKS-SIS-022	José Rivera	▸ Base de datos de los sistemas.
23	WRKS-SIS-023	José Rivera	▸ Respaldo de los pasos de datos.

Tabla 2 - Identificación de Activos

II.2.2 *AGRUPACIÓN DE ACTIVOS*

La tarea clasifica los Activos identificados en las tipologías ofrecidas por Magerit y los agrupa según:

- PC / Laptop
- Servidores
- Información / Datos
- Aplicaciones (Software)

II.2.3 *DIMENSIONES DE VALORACIÓN*

Son las características o atributos que hacen valioso un activo. Una dimensión es una faceta o aspecto de un activo, independiente de otras.

Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado con respecto a dicho aspecto.

- **Disponibilidad [D].-** Disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.

- **Integridad [I].-** Mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización.

- **Confidencialidad [C].-** Que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos.

II.2.4 *CRITERIOS DE VALORACIÓN*

Para valorar los activos, la siguiente escala de valores nos ofrece los siguientes aspectos:

- Escala común para todas las dimensiones, permitiendo comparar riesgos.
- Escala logarítmica, centrada en diferencias relativas de valor.
- Criterio homogéneo que permita comparar análisis realizados por separado.

Se ha elegido una escala detallada de diez valores, dejando en valor 0 como determinante de lo que sería un valor sin relevancia alguna:

ESCALAS DE VALORES		
VALOR		**CRITERIO**
10	**Muy alto**	Daño muy grave a la organización.
7 a 9	**Alto**	Daño grave a la organización.
4 a 6	**Medio**	Daño importante a la organización.
1 a 3	**Bajo**	Daño menor a la organización.
0	**Ninguno**	Irrelevante a efectos prácticos.

Tabla 3 - Escala de Valores

Lo más normal es que un activo reciba una simple valoración en cada dimensión en la que es preciso. Este planteamiento puede y debe ser enriquecido en el caso de dimensiones más complejas, como es el caso de la disponibilidad, en la que las consecuencias varían dependiendo del tiempo que dure la interrupción. En estos casos, la dimensión no recibe una única calificación, sino tantas como escalones se hayan considerado relevantes.

Los criterios que siguen se aplican en cada escalón, pudiendo variar el motivo:

CRITERIOS DE VALORIZACIÓN		
VALOR	**CRITERIO**	
10	**[olm]**	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.
	[iio]	Probablemente cause daños excepcionalmente graves a misiones extremadamente importantes de inteligencia o información.
	[si]	**Seguridad:** Probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios.
	[ir]	Probablemente cause un impacto excepcionalmente grave en las relaciones internacionales.
	[lbl]	Datos clasificados como secretos.
9	**[da]**	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización.
	[adm]	**Administración y gestión:** Probablemente impediría seriamente la operación efectiva de la organización, pudiendo llegar a su cierre.
	[lg]	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones.
	[lg.a]	Las relaciones con otras organizaciones.
	[lg.b]	Las relaciones con otros países.
	[olm]	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística.
	[iio]	Probablemente cause serios daños a misiones muy importantes de inteligencia o información.
	[cei]	**Intereses comerciales o económico:**
	[cei.a]	De enorme interés para la competencia.
	[cei.b]	De muy elevado valor comercial.

	[cei.c]	Causa de pérdidas económicas excepcionalmente elevadas.
	[cei.d]	Causa de muy significativas ganancias o ventajas para individuos u organizaciones.
	[cei.e]	Constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros.
	[lro]	**Obligaciones legales:** Probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación.
	[si]	**Seguridad:** Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios.
	[ir]	Probablemente cause un serio impacto en las relaciones internacionales.
	[lbl]	Datos clasificados como reservados.
8	**[crm]**	Impida la investigación de delitos graves o facilite su comisión.
	[lbl]	Datos clasificados como confidenciales.
7	**[da]**	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones.
	[adm]	**Administración y gestión:** probablemente impediría la operación efectiva de la organización.
	[olm]	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística.
	[iio]	Probablemente cause serios daños a misiones importantes de inteligencia o información.
	[cei]	**Intereses comerciales o económico:**
	[cei.a]	De enorme interés para la competencia.
	[cei.b]	De muy elevado valor comercial.
	[cei.c]	Causa de pérdidas económicas excepcionalmente elevadas.
	[cei.d]	Causa de muy significativas ganancias o ventajas para individuos u organizaciones.

	[cei.e]	Constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros.
	[lro]	**Obligaciones legales:** Probablemente cause un incumplimiento grave de una ley o regulación.
	[si]	**Seguridad:** Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.
	[ir]	Probablemente cause un impacto significativo en las relaciones internacionales.
	[lbl]	Datos clasificados como confidenciales.
6	**[pi1]**	**Información personal:** Probablemente afecte gravemente a un grupo de individuos.
	[pi2]	**Información personal:** Probablemente quebrante seriamente la ley o algún reglamento de protección de información personal.
	[ps]	**Seguridad de las personas**: probablemente cause daños de cierta consideración, restringidos a un individuo.
	[po]	**Orden público:** probablemente cause manifestaciones, o presiones significativas.
	[lbl]	Datos clasificados como de difusión limitada.
5	**[da]**	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones.
	[adm]	**Administración y gestión:** probablemente impediría la operación efectiva de más de una parte de la organización.
	[lg]	Probablemente sea causa una cierta publicidad negativa.
	[lg.a]	Por afectar negativamente a las relaciones con otras organizaciones.
	[lg.b]	Por afectar negativamente a las relaciones con el público.
	[olm]	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local.
	[iio]	Probablemente dañe a misiones importantes de inteligencia o información.

	[pi1]	**Información personal:** Probablemente afecte gravemente a un individuo.
	[pi2]	**Información personal:** Probablemente quebrante seriamente leyes o regulaciones.
	[lro]	**Obligaciones legales:** Probablemente sea causa de incumplimiento de una ley o regulación.
	[ir]	Probablemente tenga impacto en las relaciones internacionales.
	[lbl]	Datos clasificados como de difusión limitada.
4	**[pi1]**	**Información personal:** Probablemente afecte a un grupo de individuos.
	[pi2]	**Información personal:** Probablemente quebrante leyes o regulaciones.
	[ps]	**Seguridad de las personas:** Probablemente cause daños menores a varios individuos.
	[crm]	Dificulte la investigación o facilite la comisión de delitos.
	[lbl]	Datos clasificados como de difusión limitada.
3	**[da]**	Probablemente cause la interrupción de actividades propias de la Organización.
	[adm]	**Administración y gestión:** Probablemente impediría la operación efectiva de una parte de la organización.
	[lg]	Probablemente afecte negativamente a las relaciones internas de la Organización.
	[olm]	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local).
	[iio]	Probablemente cause algún daño menor a misiones importantes de inteligencia o información.
	[cei]	**Intereses comerciales o económicos:**
	[cei.a]	De cierto interés para la competencia.
	[cei.b]	De cierto valor comercial.
	[cei.c]	Causa de pérdidas financieras o merma de ingresos.

	[cei.d]	Facilita ventajas desproporcionadas a individuos u organizaciones.
	[cei.e]	Constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros.
	[pi1]	**Información personal:** Probablemente afecte a un individuo.
	[pi2]	**Información personal:** Probablemente suponga el incumplimiento de una ley o regulación.
	[lro]	**Obligaciones legales:** Probablemente sea causa de incumplimiento leve o técnico de una ley o regulación.
	[si]	**Seguridad:** Probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente.
	[ps]	**Seguridad de las personas:** Probablemente cause daños menores a un individuo.
	[po]	**Orden público:** Causa de protestas puntuales.
	[ir]	Probablemente cause un impacto leve en las relaciones internacionales.
	[lbl]	Datos clasificados como de difusión limitada.
2	**[lg]**	Probablemente cause una pérdida menor de la confianza dentro de la Organización.
	[cei]	**Intereses comerciales o económicos:**
	[cei.a]	De bajo interés para la competencia.
	[cei.b]	De bajo valor comercial.
	[pi1]	**Información personal:** Pudiera causar molestias a un individuo.
	[pi2]	**Información personal:** Pudiera quebrantar de forma leve leyes o regulaciones.
	[ps]	**Seguridad de las personas:** Pudiera causar daño menor a varios individuos.
	[lbl]	Datos sin clasificar.
1	**[da]**	Pudiera causar la interrupción de actividades propias de la Organización.

	[adm]	**Administración y gestión:** Pudiera impedir la operación efectiva de una parte de la organización.
	[lg]	Pudiera causar una pérdida menor de la confianza dentro de la Organización.
	[olm]	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local).
	[iio]	Pudiera causar algún daño menor a misiones importantes de inteligencia o información.
	[cei]	**Intereses comerciales o económicos:**
	[cei.a]	De pequeño interés para la competencia.
	[cei.b]	De pequeño valor comercial.
	[pi1]	**Información personal:** Pudiera causar molestias a un individuo.
	[lro]	**Obligaciones legales: P**udiera causar el incumplimiento leve o técnico de una ley o regulación.
	[si]	**Seguridad:** Pudiera causar una perjuicio en la seguridad o dificultar la investigación de un incidente.
	[ir]	Pudiera tener un impacto leve en las relaciones internacionales.
	[lbl]	Datos clasificados como sin clasificar.
0	**[1]**	No afectaría a la seguridad de las personas.
	[2]	Sería causa de inconveniencias mínimas a las partes afectadas.
	[3]	Supondría pérdidas económicas mínimas.
	[4]	No supondría daño a la reputación o buena imagen de las personas u organizaciones.

Tabla 4 - Justificación

II.2.5 *VALORACIÓN DE ACTIVOS*

Nombre del Activo	Disponibilidad		Integridad		Confidencialidad		Valor Total
	Valor	Justificación	Valor	Justificación	Valor	Justificación	
WRKS-REC-001	8	[crm]	9	[adm]	8	[lbl], [crm]	8
WRKS-REC-002	10	[olm]	5	[olm]	6	[lbl]	7
WRKS-PRE-003	3	[adm], [da]	2	[lg]	0	[4]	2
WRKS-RHH-004	7	[da]	7	[adm]	8	[lbl], [crm]	7
WRKS-CON-005	10	[olm]	10	[iio]	8	[lbl], [crm]	9
WRKS-CON-006	8	[crm]	10	[iio]	10	[lbl]	9
WRKS-CON-007	10	[olm]	10	[iio]	10	[lbl]	10
WRKS-PRO-008	10	[olm]	10	[iio]	10	[lbl]	10
WRKS-PRO-009	6	[pi1]	10	[iio]	9	[lbl]	8
WRKS-PRO-010	10	[olm]	10	[iio]	8	[lbl], [crm]	9
WRKS-PRO-011	10	[olm]	10	[iio]	10	[lbl]	10
WRKS-PRO-012	8	[crm]	10	[iio]	10	[lbl]	9
WRKS-PRO-024	7	[da]	7	[adm]	7	[lbl]	7
WRKS-PRO-013	10	[olm]	10	[iio]	3	[lbl]	8
WRKS-SEL-014	10	[olm]	10	[iio]	4	[lbl]	8
WRKS-IMP-015	10	[olm]	10	[iio]	10	[lbl]	10
WRKS-CAL-017	6	[pi1]	5	[olm]	8	[lbl], [crm]	6
WRKS-EXT-016	5	[adm], [da]	5	[olm]	5	[lbl]	5
WRKS-CAL-018	5	[adm]	7	[adm]	3	[lbl]	5
WRKS-BOD-019	10	[olm]	8	[crm]	10	[lbl]	9
WRKS-BOD-020	5	[adm], [da]	5	[olm]	5	[lbl]	5
WRKS-SIS-022	10	[olm]	10	[iio]	10	[lbl]	10
WRKS-SIS-023	3	[adm], [da]	3	[iio], [olm]	3	[lbl]	3

Tabla 5 - Valoración de Activos

II.3 IDENTIFICAR AMENAZAS Y VULNERABILIDADES

Se denomina vulnerabilidad a la exposición latente a un riesgo en el área de informática, de los cuales podrían ser del tipo lógica, como físico; no obstante, con la adopción de nuevos medios tecnológicos y de comunicación, los riesgos evolucionan y las conexiones se hacen menos seguras cada vez.

La definición de amenaza está dada como un evento que puede ocurrir, producto de un daño sobre los elementos de un sistema, las cuales pueden afectar, ya sea a la integridad, disponibilidad, confidencialidad y autenticidad de los datos e información con técnicas tales como: el reconocimiento de puntos de entrada, fronteras de privilegios y árboles de amenazas, se pueden identificar estrategias para mitigar las posibles amenazas.

Es importante considerar que las amenazas permanecen siempre latentes y las vulnerabilidades no desaparecerán en su totalidad; por lo que los niveles de inversión en el área de seguridad en cualquier empresa deberán ir acorde a la importancia de la información en riesgo.

II.3.1 *AMENAZAS POR ACTIVO*

Activo	Amenaza		Vulnerabilidad
PC / LAPTOP	[N.1]	Incendios.	Falta de protección contra fuego.
	[N.2]	Inundaciones.	Falta de protección física adecuada.
	[N.3]	Otro desastre natural.	Condiciones locales donde los recursos son fácilmente afectados por desastres.
	[I.3]	Contaminación mecánica.	Falta de mantenimiento.
	[I.4]	Avería de origen físico.	Falta de mantenimiento.
	[I.5]	Corte del suministro eléctrico.	Funcionamiento no confiable del UPS.
	[I.6]	Condiciones inadecuadas de temperatura y/o humedad.	Funcionamiento no adecuado del aire acondicionado.
	[E.15]	Errores de mantenimiento /Actualización de equipos (hardware).	Falta de control.

	[A.17]	Robo.	Falta de protección física.
SERVIDOR	[N.1]	Incendios.	Falta de protección contra fuego.
	[N.2]	Inundaciones.	Falta de protección física adecuada.
	[N.3]	Otro desastre natural.	Condiciones locales donde los recursos son fácilmente afectados por desastres.
	[I.3]	Contaminación mecánica.	Falta de mantenimiento.
	[I.4]	Avería de origen físico.	Falta de mantenimiento.
	[I.5]	Corte del suministro eléctrico.	Funcionamiento no confiable del UPS.
	[I.6]	Condiciones inadecuadas de temperatura y/o humedad.	Funcionamiento no adecuado del aire acondicionado.
	[E.15]	Errores de mantenimiento /Actualización de equipos (hardware).	Falta de control.
	[A.17]	Robo.	Falta de protección física.
INFORMACIÓN / DATOS	[E.5]	Difusión de software dañino.	Falta de control.
	[E.9]	Introducción de información incorrecta.	Desconocimiento de la aplicación.
	[A.13]	Destrucción la información.	Falta de control.
	[E.10]	Degradación de la información.	Respaldo inadecuado.
APLICACIONES (SOFTWARE)	[E.1]	Errores del administrador.	Falta de capacitación del administrador del sistema.
	[E.2]	Errores de los usuarios.	Falta de conocimiento para el uso de la aplicación.
	[E.3]	Errores de monitorización (log).	Incapacidad de la aplicación.
	[E.9]	Introducción de información incorrecta.	Falta de conocimiento para el uso de la aplicación.
	[E.14]	Errores de mantenimiento / actualización de programas (software).	Falta de procedimientos aprobados.
	[E.16]	Caída del sistema por agotamiento de recursos.	Sobrecarga en la utilización de la aplicación.
	[A.16]	Denegación de servicio.	Incapacidad para distinguir una petición real de una petición falsificada.

Tabla 6 - Amenaza por activos

II.4 IDENTIFICAR IMPACTOS

Se considera impacto a todo hecho que se presentó y que resuelto o no, provocó algún tipo de repercusión importante (sobre todo negativa) en la funcionalidad de alguna parte de la organización; en nuestro caso específicamente a los activos físicos y toda la información que almacenan.

Estableciendo las prioridades a las diversas situaciones, se deben asignar valores a los sistemas que pueden ser afectados por las potenciales amenazas, en base a esto se pueden determinar cuáles deberían ser atendidas inmediatamente. Habrá que analizar todos los criterios de valorización, como son la confidencialidad, disponibilidad e integridad, aplicando una tabla que nos cuantificará las incidencias. Además de identificar los impactos, hay que clasificarlos dependiendo el tipo de consecuencias que las amenazas pueden producir en los activos:

IMPACTOS CON CONSECUENCIAS CUANTITATIVAS	
C1	Pérdidas económicas
C2	Pérdidas inmateriales
C3	Responsabilidad legal, civil o penal

IMPACTOS CON CONSECUENCIAS CUALITATIVAS ORGÁNICAS	
L1	Pérdida de fondos patrimoniales
L2	Incumplimiento de obligaciones legales
L3	Perturbación o situación embarazosa político-administrativa
L4	Daño a las personas

IMPACTOS CON CONSECUENCIAS CUALITATIVAS FUNCIONALES	
[C]	Confidencialidad
[I]	Integridad
[D]	Disponibilidad

Tabla 7 – Impactos

II.4.1 *IMPACTO POR AMENAZA*

ACTIVO	AMENAZA		IMPACTO	TIPOS DE CONSECUENCIAS		
				CUANTITATIVA	CUALITATIVA	FUNCIONAL
PC / LAPTOP	[N.1]	Incendios	Reduce la disponibilidad	C1, C2	L4	[D]
	[N.2]	Inundaciones	Reduce la disponibilidad	C1, C2	L4	[D]
	[N.3]	Otro desastre natural	Reduce la disponibilidad	C1, C2	L4	[D]
	[I.3]	Contaminación mecánica	Reduce la disponibilidad	C1, C2	L4	[D]
	[I.4]	Avería de origen físico	Reduce la disponibilidad	C1, C2	-	[D]
	[I.5]	Corte del suministro eléctrico	Reduce la disponibilidad	C1, C2	-	[D]
	[I.6]	Condiciones inadecuadas de temperatura y/o humedad	Reduce la disponibilidad	C1, C2	L4	[D]
	[E.15]	Errores de mantenimiento / actualización de equipos (hardware)	Reduce la disponibilidad	C1, C2	-	[D]
	[A.17]	Robo	Reduce la disponibilidad, confidencialidad	C1, C2 ,C3	L4	[D], [C]
SERVIDOR	[N.1]	Incendios	Reduce la disponibilidad	C1, C2	L4	[D]
	[N.2]	Inundaciones	Reduce la disponibilidad	C1, C2	L4	[D]
	[N.3]	Otro desastre natural	Reduce la disponibilidad	C1, C2	L4	[D]
	[I.3]	Contaminación mecánica	Reduce la disponibilidad	C1, C2	L4	[D]
	[I.4]	Avería de origen físico	Reduce la disponibilidad	C1, C2	-	[D]
	[I.5]	Corte del suministro eléctrico	Reduce la disponibilidad	C1, C2	-	[D]

	[I.6]	Condiciones inadecuadas de temperatura y/o humedad	Reduce la disponibilidad	C1, C2	L4	[D]
	[E.15]	Errores de mantenimiento / actualización de equipos (hardware)	Reduce la disponibilidad	C1, C2	-	[D]
	[A.17]	Robo	Reduce la disponibilidad, confidencialidad	C1, C2 ,C3	L4	[D], [C]
INFORMACIÓN / DATOS	[E.5]	Difusión de software dañino	Reduce la disponibilidad, confidencialidad e integridad	C2	L1	[D], [C], [I]
	[E.9]	Introducción de información incorrecta	Reduce la integridad	C1,C2	L3	[I]
	[A.13]	Destrucción la información	Reduce la disponibilidad	C1, C2	L1	[D]
	[E.10]	Degradación de la información	Reduce la integridad	C2	L1	[I]
APLICACIONES (SOFTWARE)	[E.1]	Errores del administrador	Reduce la disponibilidad, confidencialidad e integridad	C2	L3	[D], [C], [I]
	[E.2]	Errores de los usuarios	Reduce la disponibilidad e integridad	C2	-	[D], [I]
	[E.3]	Errores de monitorización (log)	Reduce la confidencialidad	C2	-	[C]
	[E.9]	Introducción de información incorrecta	Reduce la integridad	C1, C2	L3	[I]
	[E.14]	Errores de mantenimiento / actualización de programas (software)	Reduce la disponibilidad e integridad	C2	L3	[D], [I]
	[E.16]	Caída del sistema por agotamiento de recursos	Reduce la disponibilidad	C1, C2	L1, L3	[D]
	[A.16]	Denegación de servicio	Reduce la disponibilidad	C2	-	[D]

Tabla 8 - Impacto por amenaza

II.5 ANÁLISIS Y EVALUACIÓN DE RIESGOS

Se dedica a identificar las amenazas, vulnerabilidades y riesgos a los que están expuestos los equipos, sobre el entorno de trabajo y tecnológico de la organización; y posteriormente generar un plan de implementación de los controles que aseguren un ambiente informático seguro, bajo los criterios de disponibilidad, confidencialidad e integridad de la información.

Las dimensiones de valoración están dadas en base a la fuente de la amenaza, su capacidad y la naturaleza de la vulnerabilidad. Con la finalidad de poder establecer las medidas preventivas a aplicarse, es necesario identificar los riesgos en todas las instalaciones de la empresa y determinar una evaluación de éstos en función a las consecuencias que puedan ocasionar.

Es siguiente cuadro muestra nos muestra más detallado un análisis y evaluación de Riesgo de la empresa Plásticos Internaciones C.A.:

Los criterios de valoración de Frecuencia son los siguientes:

Frecuencia	
Casi nunca	1
Algunas veces	2
A menudo	3
Casi siempre	4
Siempre	5

Tabla 9 – Frecuencia

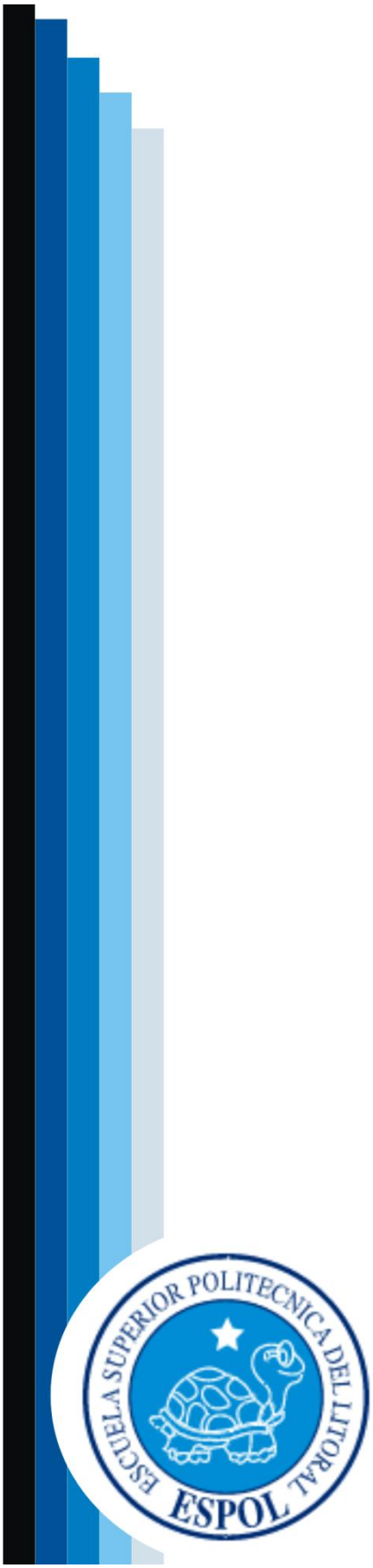
Los criterios de valoración del Impacto son los siguientes:

Impacto	
Muy Bajo	1
Bajo	2
Medio	3
Alta	4
Muy alto	5

Tabla 10 - Impacto

ACTIVO		AMENAZA	FRECUENCIA	IMPACTO	VALOR DEL RIESGO
PC / Laptop	[N.1]	Incendios	1	5	5
	[N.2]	Inundaciones	1	4	4
	[N.3]	Otro desastre natural	1	5	5
	[I.3]	Contaminación mecánica	3	3	9
	[I.4]	Avería de origen físico	1	2	2
	[I.5]	Corte del suministro eléctrico	4	5	20
	[I.6]	Condiciones inadecuadas de temperatura y/o humedad	1	3	3
	[E.15]	Errores de mantenimiento / actualización de equipos (hardware)	3	3	9
	[A.17]	Robo	1	5	5
Servidor	[N.1]	Incendios	1	5	5
	[N.2]	Inundaciones	1	4	4
	[N.3]	Otro desastre natural	1	5	5
	[I.3]	Contaminación mecánica	3	3	9
	[I.4]	Avería de origen físico	1	2	2
	[I.5]	Corte del suministro eléctrico	4	5	20
	[I.6]	Condiciones inadecuadas de temperatura y/o humedad	1	3	3
	[E.15]	Errores de mantenimiento / actualización de equipos (hardware)	3	3	9
	[A.17]	Robo	1	5	5
Información / Datos	[E.5]	Difusión de software dañino	3	4	12
	[E.9]	Introducción de información incorrecta	3	3	9
	[A.13]	Destrucción la información	3	5	15
	[E.10]	Degradación de la información	1	4	4
Aplicaciones (Software)	[E.1]	Errores del administrador	3	3	9
	[E.2]	Errores de los usuarios	4	3	12
	[E.3]	Errores de monitorización (log)	1	1	1
	[E.9]	Introducción de información incorrecta	3	3	9
	[E.14]	Errores de mantenimiento / actualización de programas (software)	3	2	6
	[E.16]	Caída del sistema por agotamiento de recursos	2	4	8
	[A.16]	Denegación de servicio	1	1	1

Tabla 11 - Análisis y evaluación de riesgo



CAPÍTULO III

EJECUCIÓN DEL SGSI

III. EJECUCIÓN DEL SGSI

III.1 DEFINIR PLAN DE TRATAMIENTO DE RIESGO

El Plan de Tratamiento de Riesgos (PTR) consiste en seleccionar y aplicar las medidas más adecuadas, con el fin de poder modificar el riesgo para evitar los daños intrínsecos al factor de riesgo, o bien aprovechar las ventajas que pueda reportarnos.

III.1.1 *OPCIONES PARA EL TRATAMIENTO DEL RIESGO*

Para el tratamiento del riesgo existen cuatro estrategias:

Reducción del Riesgo

Se deben implementar los apropiados controles para disminuirlos a los niveles de aceptación previamente identificados por la empresa.

Los controles pueden reducir los riesgos valorados en varias maneras:

- Reduciendo la posibilidad de que la vulnerabilidad sea explotada por las amenazas.
- Reduciendo la posibilidad de impacto si el riesgo ocurre detectando eventos no deseados, reaccionando o recuperándose de ellos.

La selección de cualquiera de estas maneras para controlar los riesgos dependerá de una serie de factores, tales como: requerimientos comerciales de la organización, el ambiente, y las circunstancias en que la firma requiere operar.

Aceptación del Riesgo

Es probable que a la empresa se le presente situaciones donde no se pueden encontrar controles ni tampoco es viable diseñarlos o el costo de implantar el control es mayor que las consecuencias del riesgo. En estas circunstancias una decisión razonable pudiera ser la de inclinarse por la aceptación del riesgo, y vivir con las consecuencias si el riesgo ocurriese.

Transferencia del Riesgo

Es una opción para la empresa, cuando es muy difícil, tanto técnica como económicamente para la organización llevar al riesgo a un nivel aceptable. En estas circunstancias podría ser económicamente factible, transferir el riesgo a una aseguradora.

Hay que tomar en cuenta, que con las empresas aseguradoras, siempre existe un elemento de riesgo residual. Siempre existen condiciones con las aseguradoras de exclusiones, las cuales se aplicarán dependiendo del tipo de ocurrencia, bajo la cual no se provee una indemnización. La transferencia del riesgo por lo tanto, debe ser muy bien analizada para así poder identificar con precisión, cuánto del riesgo actual está siendo transferido. Lo que debe estar claro, es que al tercerizar servicios, el riesgo residual no se delega, es responsabilidad de la empresa.

Evitar el Riesgo

La opción de evitar el riesgo, describe cualquier acción donde las actividades del negocio, o las maneras de conducir la gestión comercial del negocio, se modifican, para así poder evitar la ocurrencia del riesgo.

Las maneras habituales para implementar esta opción son:

- Dejar de conducir ciertas actividades.
- Desplazar activos de información de un área riesgosa a otra.
- Decidir no procesar cierto tipo de información si no se consigue la protección adecuada.

La decisión por la opción de “evitar el riesgo” debe ser balanceada contra las necesidades financieras y comerciales de la empresa.

III.2 IMPLEMENTAR PLAN DE TRATAMIENTO DE RIESGO

Los controles seleccionados basados en Gestión de Activos son los siguientes:

ACTIVO	AMENAZA		VULNERABILIDAD	PTR
PC / LAPTOP	[I.3]	Contaminación mecánica	Falta de mantenimiento	Reducción
	[I.5]	Corte del suministro eléctrico	Funcionamiento no confiable del UPS	Reducción
	[E.15]	Errores de mantenimiento / actualización de equipos (hardware)	Falta de control	Reducción
SERVIDORES	[I.3]	Contaminación mecánica	Falta de mantenimiento	Reducción
	[I.5]	Corte del suministro eléctrico	Funcionamiento no confiable del UPS	Reducción
INFORMACIÓN / DATOS	[E.5]	Difusión de software dañino	Falta de control	Reducción
	[E.9]	Introducción de información incorrecta	Desconocimiento de la aplicación	Reducción
	[A.13]	Destrucción la información	Falta de Protección Anti-Virus actualizada	Reducción
APLICACIONES (SOFTWARE)	[E.1]	Errores del administrador	Falta de capacitación del administrador del sistema	Reducción
	[E.2]	Errores de los usuarios	Falta de conocimiento para el uso de la aplicación	Reducción
	[E.9]	Introducción de información incorrecta	Falta de conocimiento para el uso de la aplicación	Reducción

Tabla 12 - Implementar plan de tratamiento de riesgo

Ya realizado el PTR sobre la organización, se deberá de reconocer que por más eficiente que sea el PTR, existirá siempre un riesgo residual. El riesgo residual es aquel riesgo que queda en la empresa después de un arduo análisis de seguridad a través de un PTR. El riesgo residual no tiene proporciones ni estándares; es un estimado que está en función del PTR que lleva la empresa para salvar su información.

III.2.1 *CONTROLES SELECCIONADOS DE LA NORMA ISO 27002*

La norma ISO 27002 nos ofrece los controles más apropiados para reducir todos estos riesgos excesivos identificados. Los controles seleccionados son los siguientes:

ACTIVO	AMENAZA		VULNERABILIDAD	PTR
PC / Laptop	[I.3]	Contaminación mecánica	Falta de mantenimiento	**9.2.1** Ubicación y protección de los equipos.
				7.1.3 Uso aceptable de los equipos.
				9.2.4 Mantenimiento de equipos.
	[I.5]	Corte del suministro eléctrico	Funcionamiento no confiable del UPS	**9.2.9.2** Servicios de Suministro.
				14.1 Aspectos de la seguridad de la información de la gestión de la continuidad del negocio.
				14.1.3 Desarrollar e implementar los planes de continuidad incluyendo la seguridad de la información.
				14.1.5 Prueba, mantenimiento y re-evaluación de los planes de continuidad del negocio.
	[E.15]	Errores de mantenimiento / actualización de equipos (hardware)	Falta de control	**9.2.4** Mantenimiento de equipos.
				13.2.1 Responsabilidades y procedimientos
				8.2.2 Conocimiento, educación y capacitación en seguridad de la información.
	[I.3]	Contaminación mecánica	Falta de mantenimiento	**9.2.4** Mantenimiento de equipos.
	[I.5]	Corte del	Funcionamiento no	**9.2.9.2** Servicios de

		suministro eléctrico	confiable del UPS	Suministro.
				14.1 Aspectos de la seguridad de la información de la gestión de la continuidad del negocio.
				14.1.3 Desarrollar e implementar los planes de continuidad incluyendo la seguridad de la información.
				14.1.5 Prueba, mantenimiento y re-evaluación de los planes de continuidad del negocio.
Información / Datos	**[E.5]**	Difusión de software dañino	Falta de Antivirus o desactualización	**10.4.1** Controles contra códigos maliciosos.
				10.4.2 Controles contra códigos móviles.
				10.5 Respaldo o Back-Up.
	[E.9]	Introducción de información incorrecta	Desconocimiento de la aplicación	**8.1.1** Roles y responsabilidades.
				8.2.2 Conocimiento, educación y capacitación en seguridad de la información.
				13.1 Reporte de los eventos y debilidades de la seguridad de la información.
	[A.13]	Destrucción la información	Falta de control	**13.1** Reporte de los eventos y debilidades de la seguridad de la información.
				8.2.2 Conocimiento, educación y capacitación en seguridad de la información.

Aplicaciones (Software)	**[E.1]**	Errores del administrador	Falta de capacitación del administrador del sistema	**13.2.1** Responsabilidades y procedimientos.
	[E.2]	Errores de los usuarios	Falta de conocimiento para el uso de la aplicación	**13.1** Reporte de los eventos y debilidades de la seguridad de la información.
				5.1 Política de seguridad de la información.
				5.1.1 Documento de política de seguridad de la información.
				15.1 Cumplimiento con los requisitos legales.
	[E.9]	Introducción de información incorrecta	Falta de conocimiento para el uso de la aplicación	**15.1.4** Protección de los datos y de la privacidad de la información personal.

Tabla 13 - Control de Selecciones de la norma ISO 27002

III.2.2 *SALVAGUARDAS*

Las salvaguardas permiten hacer frente a las amenazas. Hay diferentes aspectos en los cuales puede actuar una salvaguarda para alcanzar sus objetivos de limitación del impacto y/o mitigación del riesgo:

Procedimientos: Que siempre son necesarios; a veces bastan procedimientos, pero otras veces son un componente de una salvaguarda más compleja. Se requieren procedimientos tanto para la operación de las salvaguardas preventivas como para la gestión de incidencias y la recuperación tras las mismas.

Política de personal: Que es necesaria cuando se consideran sistemas atendidos por personal.

Soluciones técnicas: Frecuentes en el entorno de las tecnologías de la información, que pueden ser:

- Aplicaciones (software)
- Dispositivos físicos
- Protección de las comunicaciones
- Seguridad física, de los locales y áreas de trabajo

III.3 IMPLEMENTAR LOS CONTROLES

Una vez seleccionado los controles procedemos a su implementación:

III.3.1 *CONTROLES Y POLÍTICAS DE SEGURIDAD*

GENERALIDADES

La seguridad informática ha tenido un gran incremento, debido a las nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar más en el ambiente internacional, lo cual lógicamente ha traído consigo la aparición de nuevas amenazas para los sistemas de información. Estos riesgos que se enfrentan han llevado a que se desarrolle un documento de Políticas de Seguridad que orienten el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de la mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la compañía Plásticos Internacionales C.A.

En este sentido, las políticas de seguridad informática definidas partiendo desde el análisis de los riesgos a los que se encuentra propensa la compañía surgen como una herramienta organizacional para concienciar a los colaboradores de la organización sobre la importancia y sensibilidad de la información; y servicios críticos que permiten a la empresa crecer y mantenerse competitiva.

Ante esta situación, el proponer nuestra política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades

en su aplicación, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea la compañía.

ALCANCE DE LAS POLÍTICAS

Este manual de políticas de seguridad es elaborado de acuerdo al análisis de riesgos y de vulnerabilidades encontradas a lo largo del estudio, por consiguiente el alcance de estas políticas, se encuentra sujeto a la empresa.

OBJETIVOS

Desarrollar un sistema de seguridad significa "planear, organizar, dirigir y controlar las actividades para mantener y garantizar la integridad física de los recursos informáticos, así como resguardar los activos de la empresa".

Los objetivos que se desean alcanzar luego de implantar nuestro sistema de seguridad son los siguientes:

- Establecer un esquema de seguridad con perfecta claridad y transparencia bajo la responsabilidad de la compañía en la administración del riesgo.
- Compromiso de todo el personal de la compañía con el proceso de seguridad, agilizando la aplicación de los controles con dinamismo y armonía.
- Que la prestación del servicio de seguridad gane en calidad.
- Todos los empleados se convierten en interventores del SGSI.

III.3.2 *DEFINICIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA*

En esta sección del documento se presenta una propuesta de políticas de seguridad, como un recurso para mitigar los riesgos a los que la compañía se ve expuesta.

DISPOSICIONES GENERALES

Artículo 1º

El presente ordenamiento tiene por objeto estandarizar y contribuir al desarrollo informático de las diferentes áreas de la compañía. Para los efectos de este instrumento se entenderá por:

COMITÉ

Al equipo integrado por la Gerencia, los Jefes de área y el personal administrativo (ocasionalmente) convocado para fines específicos como:

- Adquisiciones de Hardware y software.
- Establecimiento de estándares de la Compañía Plásticos Internacionales tanto de hardware como de software.
- Establecimiento de la Arquitectura Tecnológica.
- Establecimiento de lineamientos para concursos de ofertas.
- Administración de informática.

Está integrada por la Gerencia y Jefes de área, las cuales son responsables de:

- Velar por el funcionamiento de la tecnología informática que se utilice en las diferentes áreas.
- Elaborar y efectuar seguimiento del Plan Maestro de Informática.
- Definir estrategias y objetivos a corto, mediano y largo plazo.
- Mantener la Arquitectura tecnológica.
- Controlar la calidad del servicio brindado.
- Mantener el Inventario actualizado de los recursos informáticos.
- Velar por el cumplimiento de las Políticas y Procedimientos establecidos.

Para los efectos de este documento, se entiende por Políticas en Informática, al conjunto de reglas obligatorias, que deben observar los Jefes de Sistemas responsables del hardware y software existente en la compañía, siendo responsabilidad de la Administración de Informática, vigilar su estricto cumplimiento en el ámbito de su competencia, tomando las medidas preventivas y correctivas para que se cumplan.

Artículo 2º

Las Políticas en Informática son el conjunto de ordenamientos y lineamientos enmarcados en el ámbito jurídico y administrativo. Estas normas inciden en la

adquisición y el uso de los Bienes y Servicios Informáticos, las cuales se deberán de acatar invariablemente, por aquellas instancias que intervengan directa y/o indirectamente en ello.

Artículo 3º

La compañía deberá contar con un Jefe o responsable, en el que recaiga la administración de los Bienes y Servicios, que vigilará la correcta aplicación de los ordenamientos establecidos por el Comité y demás disposiciones aplicables.

IDENTIFICACIÓN DE LOS EQUIPOS DE CÓMPUTO

Artículo 4º

Se identificarán los activos importantes asociados a cada sistema de información, sus respectivos propietarios, para luego elaborar un inventario con dicha información. La identificación de los activos físicos de la empresa se los realizará en el siguiente formato:

Área	-	**Responsable**	-
		Cargo	-
Nombre del Equipo	-		

	CPU
Serie No.	-
Marca	-
Memoria RAM	-
Disco Duro	-
Procesador	-
Sistema Operativo	-

	Monitor	**Mouse**	**Teclado**	**Impresora**
Serie No.	-	-	-	-
Marca	-	-	-	-
Modelo No.	-	-	-	-

Observación	-

Tabla 14 - Formato de Inventario

INSTALACIONES DE LOS EQUIPOS DE CÓMPUTO

Artículo 5º

La instalación del equipo de cómputo, quedará sujeta a los siguientes lineamientos:

- Los equipos para uso interno se instalarán en lugares adecuados, lejos de polvo y tráfico de personas.
- La Administración de Informática, así como las áreas operativas deberán contar con un croquis actualizado de las instalaciones eléctricas y de comunicaciones del equipo de cómputo en red.
- Las instalaciones eléctricas y de comunicaciones, estarán de preferencia fija o en su defecto resguardadas del paso de personas o máquinas, y libres de cualquier interferencia eléctrica o magnética.
- Las instalaciones se apegarán estrictamente a los requerimientos de los equipos, cuidando las especificaciones del cableado y de los circuitos de protección necesarios.
- En ningún caso se permitirán instalaciones improvisadas o sobrecargadas.

La supervisión y control de las instalaciones se llevará a cabo en los plazos y mediante los mecanismos que establezca el Comité.

FUNCIONAMIENTO DE LOS EQUIPOS DE CÓMPUTO

Artículo 6º

Es obligación de la Administración de Informática vigilar que el equipo de cómputo se use bajo las condiciones especificadas por el proveedor y de acuerdo a las funciones del área a la que se asigne.

Artículo 7º

Los colaboradores de la empresa al usar el equipo de cómputo, se abstendrán de consumir alimentos, fumar o realizar actos que perjudiquen el funcionamiento del mismo o deterioren la información almacenada.

Artículo 8º

Mantener pólizas de seguros de los recursos informáticos en funcionamiento.

Artículo 9º

En ningún caso se autorizará la utilización de dispositivos ajenos a los procesos informáticos del área. Por consiguiente, se prohíbe el ingreso y/o instalación de hardware y software particular, es decir que no sea propiedad de la compañía, excepto en casos emergentes que la Dirección autorice.

ANTIVIRUS

Artículo 10º

En todos los equipos de la empresa se debe instalar y correr el antivirus actualizado, el mismo que debería cumplir con lo siguiente:

- Detectar y controlar cualquier acción intentada por un software viral en tiempo real.
- Periódicamente ejecutar el Análisis para detectar software viral almacenado en la estación de trabajo.
- Hacer una revisión al menos diaria para actualizar la definición del software antivirus.
- Debe ser un producto totalmente legal (con licencia o Software libre).

No deben usarse memorias extraíbles u otros medios de almacenamiento en cualquier computadora de la empresa a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos. Deberá existir un procedimiento formal a seguir en caso que se detecte un virus en algún equipo del sistema.

DISPOSITIVOS DE SOPORTE

Artículo 11º

Deberán existir los siguientes dispositivos de soporte en la empresa:

- **Aire acondicionado:** en el centro de cómputos la temperatura debe mantenerse entre 19º C y 20º C.
- **Matafuegos:** deberán ser dispositivos químicos y manuales que cumplan las especificaciones para extinguir incendios en equipos eléctricos de computación, deberán estar instalados en lugares estratégicos de la empresa, el centro de cómputos deberá contar con uno propio ubicado en la habitación de los servidores.
- **UPS:** (Uninterruptible, power, supply) deberá existir al menos un UPS en el centro de cómputos que atienda a los servidores, con tiempo suficiente para que se apaguen de forma segura.
- **Luz de emergencia:** deberá existir una luz de emergencia que se active automáticamente ante una contingencia.
- Deberán existir procedimientos detallados a seguir por el personal en caso de emergencias, indicando responsables, quiénes deben estar adecuadamente capacitados.

RESPALDOS

Artículo 12º

Se deberá asegurar la existencia de un procedimiento aprobado para la generación de copias de resguardo sobre toda la información necesaria para las operaciones de la organización, donde se especifique la periodicidad y el lugar físico donde se deben mantener las copias generadas.

Los archivos de respaldos deben tener un control de acceso lógico de acuerdo a la sensibilidad de sus datos, además de contar con protección física.

Deben generarse copias de respaldo de las configuraciones de los servidores, documentando las modificaciones realizadas para identificar las distintas versiones. Se deberá establecer un procedimiento de emergencia para dejar sin efecto los cambios efectuados y poder recuperar las versiones autorizadas anteriores.

Se deberá generar una copia de respaldo de toda la documentación del centro de cómputos, incluyendo el hardware, el software, la cual deberá ser de acceso restringido y estar físicamente en un lugar distinto a los centros de procesamiento.

MANTENIMIENTO DE EQUIPOS

Artículo 13º

Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes, para ello se debe considerar:

- Someter el equipamiento a tareas de mantenimiento preventivo.
- El responsable del área informática mantendrá listado actualizado del equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo.
- Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
- Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.
- A continuación se indica el período aconsejable para realizar los mantenimientos de los activos:

EQUIPO	FRECUENCIA DE MANTENIMIENTO	PERSONAL AUTORIZADO
SERVIDORES	3 meses	Jefe de Sistemas
ESTACIONES DE TRABAJO	6 meses	Jefe de Sistemas
IMPRESORAS	6 meses	Jefe de Sistemas

Tabla 15 - Plan de Mantenimiento anual

USO APROPIADO DE LOS RECURSOS

Artículo 14º

Los Recursos Informáticos están disponibles exclusivamente para cumplir las obligaciones y propósito para lo que fueron diseñados e implantados. Todo el personal usuario de dichos recursos debe saber que no tiene el derecho de confidencialidad en su uso.

CONEXIONES EXTERNAS

Artículo 15º

La conectividad a Internet será otorgada para propósitos relacionados con el negocio y mediante una autorización de la Gerencia.

Debe asegurarse que la totalidad del tráfico entrante y saliente de la red interna, sea filtrado y controlado por un firewall prohibiendo el pasaje de todo el tráfico que no se encuentre expresamente autorizado.

Todas las conexiones a Internet de la empresa deben traspasar un servidor Proxy una vez que han traspasado el firewall.

PROPIEDAD DE LA INFORMACIÓN

Artículo 16º

Con el fin de mejorar la productividad, Plásticos Internacionales promueve el uso responsable de las comunicaciones en forma electrónica, en particular el teléfono, el correo de voz, el correo electrónico, y el fax. Los sistemas de comunicación y los mensajes generados y procesados por tales sistemas, incluyendo las copias de respaldo, se deben considerar como propiedad de la empresa y no propiedad de los usuarios de los servicios de comunicación.

QUEDA PROHIBIDO

Artículo 17º

El uso de estos recursos para actividades no relacionadas con el propósito de la compañía.

Artículo 18º

Las actividades, equipos o aplicaciones que no estén directamente especificados dentro de los Estándares de los Recursos Informáticos propios la compañía.

Artículo 19º

Introducir voluntariamente programas, virus, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los Recursos Informáticos.

III.4 SELECCIÓN DE CONTROLES Y SOA

Cada día surgen nuevas formas de delitos informáticos, los cuales el SGSI, tiene como objetivo proteger toda la información de relevancia en un sistema, de acuerdo con el plan establecido para la implementación de controles:

- Planificar la implantación de los controles seleccionados.
- Diseño de un Plan de Implantación: Medidas a adoptar.
- Prioridad de implantación.
- Fecha de implantación.
- Costos de implantación, Recursos necesarios (humanos, tecnológicos y económicos).
- Responsable de la implantación.
- Definir el nivel de participación necesario de las diferentes áreas. Desarrollar un Plan de Formación y Concienciación de usuarios.

CONTROLES Y RAZONES DE SELECCIÓN	
LR:	Requerimientos Legales.
CO:	Obligaciones Contractuales.
BR / BP:	Requerimientos de Negocio/Adoptar las mejores prácticas.
RRA:	Resultados de la evaluación de riesgos.

Tabla 16 – Controles y Razones

III.4.1 *DECLARACIÓN DE APLICABILIDAD (SOA)*

CONTROLES ISO 27001:2005			CONTROLES ACTUALES	OBSERVACIÓN JUSTIFICACIÓN DE EXCLUSIÓN	CONTROLES SELECCIONADOS Y LAS RAZONES PARA LA SELECCIÓN				OBSERVACIONES (DESCRIPCIÓN GENERAL DE LA APLICACIÓN)
					LR	CO	BR / BP	RRA	
CLÁUSULA	OBJETIVO DE CONTROL								
POLÍTICA DE SEGURIDAD	5.1.	Políticas de Seguridad de la Información							
	5.1.1	Documento de Política de Seguridad de la Información					■		Todos los empleados deben conocer las políticas de seguridad de la empresa
GESTIÓN DE ACTIVOS	7.1	Responsabilidad por los activos							
	7.1.1	Inventarios de Activos	■	Existe, mal formato.	■				Todos los activos deben ser claramente identificados.
	7.1.2	Propiedad de los activos	■	Existe			■		Cada activo debe tener un propietario responsable.
	7.1.3	Uso aceptables de los activos				■			Se debe implementar un manual para el uso adecuado de los activos.
	7.2	Clasificación de los activos							
	7.2.1	Lineamientos de clasificación						■	Cada información debe tener un valor dependiendo de requerimientos legales, confidencialidad y grado de crítico para la organización
	7.2.2	Etiquetado y manejo de la información					■		Se debe implementar procedimientos para manejar y clasificar la información.

SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	**8.2**	**Durante el empleo**							
	8.2.2	Conocimiento, educación y capacitación en seguridad de la información				■		■	Todos los empleados de la organización deberían recibir entrenamiento apropiado del conocimiento de los procedimientos organizacionales para la función de su trabajo.
SEGURIDAD FÍSICA Y DEL ENTORNO	**9.2**	**Seguridad de los equipos**							
	9.2.1	Ubicación y protección del equipo				■		■	El equipo debería situarse en un lugar apropiado reduciendo el riesgo de las amenazas del entorno, así como las oportunidades de acceso no autorizado.
	9.2.2	Instalaciones de suministro.					■	■	Se deberían proteger los equipos contra fallos en el suministro de energía u otras anomalías eléctricas.
	9.2.4	Mantenimiento de los equipos					■	■	Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad.
GESTIÓN DE COMUNICACIONES Y OPERACIONES	**10.4**	**Protección contra el código malicioso y móvil**							
	10.4.1	Controles contra códigos maliciosos				■	■		Se deberían implantar controles de detección y recuperación contra el software malicioso.
GESTIÓN DE INCIDENTES EN LA	**13.1**	**Reporte de los eventos y debilidades de la seguridad de la información**							
	13.2	Gestión de incidentes y mejoras de							

SEGURIDAD DE LA INFORMACIÓN		seguridad de la información							
	13.2.1	Responsabilidades y procedimientos			■		■		Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta efectiva y ordenada a los incidentes en la seguridad de información.
GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	**14.1**	**Aspectos de la seguridad de la información de la gestión de la continuidad del negocio**							
	14.1.3	Desarrollar e implementar los planes de continuidad incluyendo la seguridad de la información			■		■		Se deberían desarrollar planes de mantenimiento o recuperación de las operaciones del negocio para asegurar la disponibilidad de la información tras la interrupción o fallo de los procesos de negocio.
	14.1.5	Prueba, mantenimiento y re-evaluación de los planes de continuidad del negocio					■		Se deberían probar regularmente los planes de continuidad del negocio para garantizar su actualización y eficacia.
CUMPLIMIENTO	**15.1**	**Cumplimiento de los requerimientos legales**							
	15.1.4	Protección de la data y privacidad de la información personal			■		■		Se debería garantizar la protección y privacidad de los datos.

Tabla 17 - Declaración de Aplicabilidad (SOA)

III.5 FORMACIÓN Y CONCIENCIACIÓN

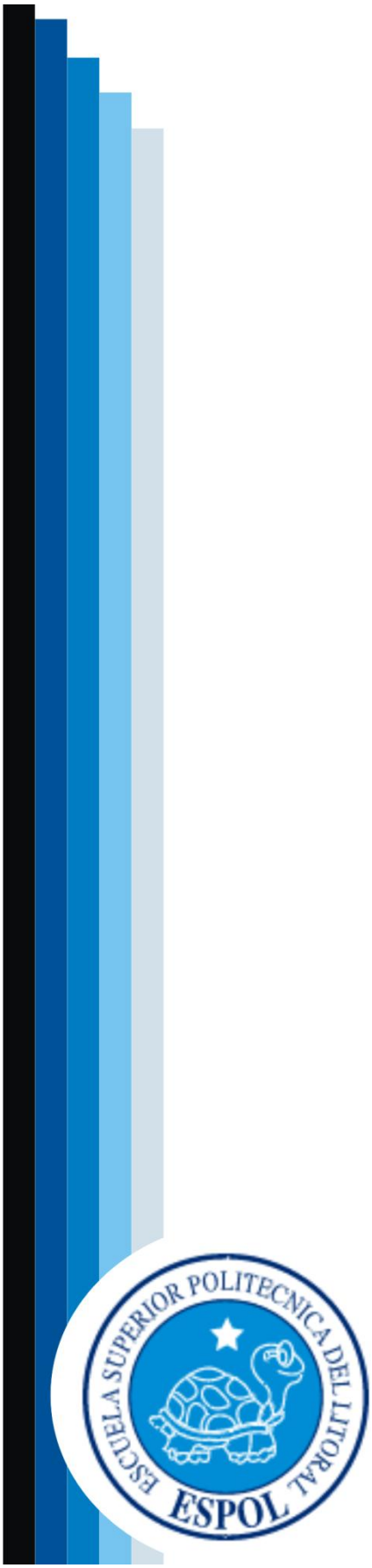
Las Políticas de Seguridad de la Información protegen de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información. Es importante que los principios de la Política de Seguridad sean parte de la cultura organizacional. Para esto, se debe asegurar un compromiso manifiesto de las máximas Autoridades del Organismo y de los titulares de Unidades Organizativas para la difusión, consolidación y cumplimiento de la presente Política.

III.5.1 *CAPACITACIÓN*

Para la eficacia de las Políticas de Seguridad de la Información, todos los empleados de la empresa, y cuando sea necesario, los usuarios externos y los terceros que desempeñen funciones en la empresa deberán recibir una adecuada capacitación y actualización periódica en materia de la política de seguridad, normas y procedimientos. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general.

El responsable del área de Recursos Humanos será el encargado de coordinar las acciones de capacitación que surjan de la Política.

Cada 6 meses se revisará el material correspondiente a la capacitación, a fin de evaluar la pertinencia de su actualización, de acuerdo al estado del arte de ese momento. El personal que ingrese a la Corporación recibirá el material, indicándosele el comportamiento esperado en lo que respecta a la seguridad de la información, antes de serle otorgados los privilegios de acceso a los sistemas que correspondan. Además se otorgará una guía de usuario para que tengan un mejor conocimiento con respecto a las amenazas informáticas y sus posibles consecuencias dentro de la Corporación de tal manera que se llegue a concienciar y crear una cultura de seguridad de la información.



ANEXOS

IV. ANEXO

IV.1 DEFINICIÓN DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Es un conjunto de políticas de administración de la información, especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) utilizando la estrategia de mejora continua de calidad PDCA.

IV.2 IMPLANTACIÓN

La implantación de ISO/IEC 27001 en una organización es un proyecto que suele tener una duración entre 6 y 12 meses, dependiendo del grado de madurez en seguridad de la información. El equipo de proyecto de implantación debe estar formado por representantes de todas las áreas de la organización que se vean afectadas por el SGSI, liderado por la dirección y asesorado por consultores externos especializados en seguridad informática.

IV.3 CERTIFICACIÓN

La certificación de un SGSI es el proceso mediante el cual una entidad de certificación externa, independiente y acreditada audita el sistema, determinando su conformidad con ISO/IEC 27001, su grado de implantación real y su eficacia y, en caso positivo, emite el correspondiente certificado.

IV.4 LA SERIE ISO 27000

La seguridad de la información tiene asignada la serie 27000 dentro de los estándares ISO/IEC:

- **ISO 27000.-** Contiene la descripción general y vocabulario a ser empleado en toda la serie 27000. Se puede utilizar para tener un entendimiento más claro de la serie y la relación entre los diferentes documentos que la conforman.
- **ISO 27001.-** "Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos". Es la norma principal de requisitos de un Sistema de Gestión de Seguridad de la Información. En su Anexo A, contempla una lista con los objetivos de control y controles que desarrolla la ISO 27002.
- **ISO 27002.-** Guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información con 11 dominios, 39 objetivos de control y 133 controles.

IV.5 MODELO A SEGUIR: PDCA

PDCA (Plan, Do, Check, Act), también conocido como "Círculo de Deming o círculo de Gabo", es una estrategia de mejora continua de la calidad en cuatro pasos:

- **PLAN (PLANIFICAR).-** es una fase de diseño del SGSI, realizando la evaluación de riesgos de seguridad de la información y la selección de controles adecuados.
- **DO (HACER).-** es una fase que envuelve la implantación y operación de los controles.
- **CHECK (VERIFICAR).-** es una fase que tiene como objetivo revisar y evaluar el desempeño (eficiencia y eficacia) del SGSI.
- **ACT (MEJORAR).-** en esta fase se realizan cambios cuando sea necesario para llevar de vuelta el SGSI a máximo rendimiento.

Figura - 4 Modelo PDCA

IV.6 METODOLOGÍA: MAGERIT

Es una metodología de análisis y gestión de riesgos de los Sistemas de Información elaborada por el Consejo Superior de Administración Electrónica para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información, enfocada a las Administraciones Públicas. MAGERIT ofrece una aplicación, pilar para el análisis y gestión de riesgos de un Sistema de Información.

IV.7 DOMINIO, OBJETIVOS DE CONTROL Y CONTROLES

Gestión de activos.

Responsabilidad sobre los activos.

- Inventario de activos.
- Responsable de los activos.
- Acuerdos sobre el uso aceptable de los activos.

Clasificación de la información

- Directrices de clasificación.
- Marcado y tratamiento de la información.

IV.8 DEFINICIÓN DEL ALCANCE DEL SGSI

El documento propone alcanzar y mantener una protección adecuada de los activos (Hardware y software que contengan información) de la organización. Identificándolos y teniendo asignado un propietario responsable que estará a cargo del cuidado del activo, maximizando su ciclo de vida.

IV.9 DEFINICIÓN DE POLÍTICAS DE SEGURIDAD

IV.9.1 *UBICACIÓN Y PROTECCIÓN DEL EQUIPO (9.2.1)*

Control

Se debiera ubicar o proteger el equipo para reducir las amenazas y peligros ambientales y oportunidades para - acceso no-autorizado.

Lineamiento de implementación

Se debieran considerar los siguientes lineamientos para la protección del equipo:

- El equipo se debiera ubicar de manera que se minimice el acceso innecesario a las áreas de trabajo;
- Los medios de procesamiento de la información que manejan data confidencia debieran ubicarse de manera que se restrinja el ángulo de visión para reducir el riesgo que la información sea vista por personas no autorizadas durante su uso; y se debieran asegurar los medios de almacenaje para evitar el acceso no autorizado;
- Se debieran aislar los ítems que requieren protección especial para reducir el nivel general de la protección requerida;
- Se debieran adoptar controles para minimizar el riesgo de amenazas potenciales; por ejemplo, robo, fuego, explosivos, humo, agua (o falla en el suministro de agua), polvo, vibración, efectos químicos, interferencias en el suministro eléctrico, interferencia en las comunicaciones, radiación electromagnética y vandalismo;
- Se debieran establecer lineamientos sobre comer, beber y fumar en la proximidad de los medios de procesamiento de información;
- Se debieran monitorear las condiciones ambientales; tales como temperatura y humedad, que pudiera afectar adversamente la operación de los medios de procesamiento de la información;

- Se debiera aplicar protección contra rayos a todos los edificios y se debieran adaptar filtros de protección contra rayos a todas las líneas de ingreso de energía y comunicaciones;
- Se debieran considerar el uso de métodos de protección, como membranas de teclado, para el equipo en el ambiente industrial;
- Se debiera proteger el equipo que procesa la información confidencial para minimizar el riesgo de escape de información debido a emanación.

IV.9.2 *MANTENIMIENTO DE EQUIPO (9.2.4)*

Control

Se debiera mantener correctamente el equipo para asegurar su continua disponibilidad e integridad.

Lineamiento de implementación

Se debieran considerar los siguientes lineamientos para el mantenimiento de equipo:

- El equipo se debiera mantener en concordancia con los intervalos y especificaciones de servicio recomendados por el proveedor;
- Sólo el personal de mantenimiento autorizado debiera llevar a cabo las reparaciones y dar servicio al equipo;
- Se debieran mantener registros de todas las fallas sospechadas y reales, y todo mantenimiento preventivo y correctivo;
- Se debieran implementar los controles apropiados cuando se programa el equipo para mantenimiento, tomando en cuenta si su mantenimiento es realizado por el personal en el local o fuera de la organización; cuando sea necesario, se debiera revisar la información confidencial del equipo, o se debiera verificar al personal de mantenimiento;
- Se debieran cumplir con todos los requerimientos impuestos por las pólizas de seguros.

IV.9.3 *SERVICIOS PÚBLICOS DE SOPORTE (9.2.2)*

Control

Se debiera proteger el equipo de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos de soporte.

Lineamiento de implementación

- Todos los servicios públicos de soporte; como electricidad, suministro de agua, desagüe, calefacción/ventilación y aire acondicionado; debieran ser adecuados para los sistemas que soportan. Los servicios públicos de soporte debieran ser inspeccionados regularmente y, conforme sea apropiado, probado para asegurar su adecuado funcionamiento y para reducir cualquier riesgo por un mal funcionamiento o falla. Se debiera proveer un suministro eléctrico adecuado que esté de acuerdo a las especificaciones del fabricante del equipo.
- Se recomienda un dispositivo de suministro de energía ininterrumpido (UPS) para apagar o el funcionamiento continuo del equipo de soporta las operaciones comerciales críticas. Los planes de contingencia para la energía debieran abarcar la acción a tomarse en el caso de una falla de energía prolongada. Se debiera considerar un generador de emergencia si se requiere que el procesamiento continué en el caso de una falla de energía prolongada. Se debiera tener disponible un adecuado suministro de combustible para asegurar que el generador pueda funcionar durante un período prolongado. El equipo UPS y los generados se debieran chequear regularmente para asegurar que tengan la capacidad adecuada y para probar su concordancia con las recomendaciones del fabricante. Además, se debiera considerar al uso de múltiples fuentes de energía, si el local es grande, una subestación de energía separada.
- Se debieran colocar interruptores de energía de emergencia cerca de las salidas de emergencia en las habitaciones donde se encuentra el equipo para facilitar el cierre del paso de corriente en caso de una emergencia. Se debiera

proporcionar iluminación de emergencia en caso de una falla en la fuente de energía principal.

- El suministro de energía debiera ser estable y adecuado para suministrar aire acondicionado, equipo de humidificación y los sistemas contra-incendios (donde se utilicen). El mal funcionamiento del sistema de suministro de agua pude dañar el equipo y evitar que el sistema contra-incendios funcione adecuadamente. Se debiera evaluar e instalar, si se requiere, un sistema de alarma para detectar mal funcionamiento en los servicios públicos de soporte.

  El equipo de telecomunicaciones se debiera conectar al proveedor del servicio mediante por lo menos dos rutas para evitar que la falla en una conexión evite el desempeño de los servicios de voz. Los servicios de voz debieran ser adecuados para cumplir con los requerimientos legales de las comunicaciones de emergencia.

Otra información

Las opciones para lograr la continuidad de los suministros de energía incluyen múltiples alimentaciones para evitar que una falla en el suministro de energía.

IV.9.4 *ASPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO (14.1)*

Objetivo

Contraatacar las interrupciones a las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

Se debiera implementar el proceso de gestión de la continuidad del negocio para minimizar el impacto sobre la organización y recuperarse de la pérdidas de activos de información (lo cual puede ser resultado de, por ejemplo, desastres naturales, accidentes, fallas del equipo y acciones deliberadas) hasta un nivel aceptable a través de una combinación de controles preventivos y de recuperación. Este proceso debiera identificar los procesos comerciales críticos e integrar los requerimientos de gestión de

la seguridad de la información de la continuidad del negocio con otros requerimientos de continuidad relacionados con aspectos como operaciones, personal, materiales, transporte y medios.

Las consecuencias de los desastres, fallas en la seguridad, pérdida del servicio y la disponibilidad del servicio debieran estar sujetas a un análisis del impacto comercial. Se debieran desarrollar e implementar planes para la continuidad del negocio para asegurar la reanudación oportuna de las operaciones esenciales. La seguridad de la información debiera ser una parte integral del proceso general de continuidad del negocio, y otros procesos gerenciales dentro de la organización.

La gestión de la continuidad del negocio debiera incluir controles para identificar y reducir los riesgos, además del proceso general de evaluación de riesgos, debiera limitar las consecuencias de incidentes dañinos y asegurar que esté disponible la información requerida para los procesos comerciales.

IV.9.5 *DESARROLLAR E IMPLEMENTAR LOS PLANES DE CONTINUIDAD INCLUYENDO LA SEGURIDAD DE LA INFORMACIÓN (14.1.3)*

Control

Se debieran desarrollar e implementar planes para mantener restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción, o falla, de los procesos comerciales críticos.

Lineamiento de implementación

El proceso de planeación de la continuidad del negocio debiera considerar lo siguiente:

- Identificar y acordar todas las responsabilidades y los procedimientos de continuidad del negocio;
- Identificar la pérdida aceptable de la información y los servicios;
- Implementación de los procedimientos para permitir la recuperación y restauración de las operaciones comerciales y la disponibilidad de la

información en las escalas de tiempo requeridas; se debiera prestar particular atención a la evaluación de las dependencias comerciales internas y externas y el establecimiento de los contratos debidos;

- Los procedimientos operacionales a seguir dependiendo de la culminación de la recuperación y restauración;
- Documentación de los procesos y procedimientos acordados;
- Educación apropiada del personal en los procedimientos y procesos acordados, incluyendo la gestión de crisis;
- Prueba y actualización de los planes.

El proceso de planeación debiera enfocarse en los objetivos comerciales requeridos; por ejemplo, restaurar los servicios de comunicación específicos a los clientes en una cantidad de tiempo aceptable. Se debieran identificar los servicios y los recursos que facilitan esto; incluyendo personal, recursos de procesamiento no-información; así como los arreglos de contingencia para los medios de procesamiento de información. Estos arreglos de contingencia pueden incluir acuerdos con terceros en la forma de acuerdos recíprocos, o servicios de suscripción comercial.

Los planes de continuidad del negocio debieran tratar las vulnerabilidades organizacionales y, por lo tanto, pueden contener información confidencial que necesita protegerse apropiadamente. Las copias de los planes de continuidad del negocio se debieran almacenar en locales remotos, a una distancia suficiente para escapar de cualquier daño de un desastre en el local principal.

La gerencia debiera asegurarse que las copias de los planes de continuidad del negocio estén actualizadas y protegidas con el mismo nivel de seguridad aplicado en el local principal.

Otro material necesario para ejecutar los planes de continuidad también debiera almacenarse en el local remoto.

Si se utilizan ubicaciones temporales alternativas, el nivel de los controles de seguridad implementados en esos locales debiera ser equivalente al de los controles del local principal.

Otra información

Se debiera notar que estos planes y actividades de gestión de crisis pueden ser diferentes a los de la gestión de la continuidad del negocio; es decir, puede ocurrir una crisis que puede ser acomodada por los procedimientos gerenciales normales.

IV.9.6 *PRUEBA, MANTENIMIENTO Y RE-EVALUACIÓN DE LOS PLANES DE CONTINUIDAD DEL NEGOCIO (14.1.5)*

Control

Los planes de continuidad del negocio debieran ser probados y actualizados regularmente para asegurar que sean actuales y efectivos.

Lineamiento de implementación

Las pruebas del plan de continuidad del negocio debieran asegurar que todos los miembros del equipo de recuperación y otro personal relevante estén al tanto de los planes y su responsabilidad con la continuidad del negocio y la seguridad de la información, y que conozcan su papel cuando se invoque el plan.

El programa de pruebas para el(los) plan(es) de continuidad debieran indicar cómo y cuándo se debiera probar cada elemento del plan. Cada elemento del(los) plan(es) debiera(n) ser probado(s) frecuentemente:

- Prueba flexible de simulación (table-top testing) de varios escenarios (discutiendo los acuerdos de recuperación comercial utilizando ejemplos de interrupciones);
- Simulaciones (particularmente para capacitar a las personas en sus papeles en la gestión post-incidente/crisis).
- Prueba de recuperación técnica (asegurando que los sistemas de información puedan restaurarse de manera efectiva.

- Prueba de recuperación en el local alternativo (corriendo los procesos comerciales en paralelo con las operaciones de recuperación lejos del local principal).
- Pruebas de los medios y servicios del proveedor (asegurando que los servicios y productos provistos externamente cumplan con el compromiso contraído).
- Ensayos completos (probando que la organización, personal, equipo, medios y procesos puedan lidiar con las interrupciones).

Estas técnicas se pueden utilizar en cualquier organización. Esto se debiera aplicar de una manera que sea relevante para el plan de recuperación específico. Los resultados de las pruebas debieran ser registradas y, cuando sea necesario, se debieran tomar acciones para mejorar los planes.

Se debiera asignar la responsabilidad de las revisiones regulares de cada plan de continuidad del negocio. La identificación de los cambios en los acuerdos comerciales que aún no se reflejan en los planes de continuidad del negocio debiera realizarse mediante una actualización apropiada del plan. Este proceso formal de control de cambios debiera asegurar que los planes de actualización sean distribuidos y reforzados mediante revisiones regulares del plan completo.

Los ejemplos de los cambios que se debieran considerar cuando se actualizan los planes de continuidad del negocio son la adquisición de equipo nuevo, actualización de los sistemas y cambios en:

- Personal
- Direcciones o números de teléfonos
- Estrategia comercial
- Local, medios y recursos
- Legislación
- Contratistas, proveedores y clientes claves
- Procesos, los nuevos o los eliminados

- Riesgo (operacional y funcional)

IV.9.7 *RESPONSABILIDADES Y PROCEDIMIENTOS (13.2.1)*

Control

Se debieran establecer las responsabilidades y los procedimientos de la gerencia para asegurar una respuesta rápida, efectiva y metódica ante los incidentes de la seguridad de la información.

Lineamiento de la implementación

Además de reportar los eventos y debilidades en la seguridad de la, se debiera utilizar el monitoreo del sistema, alertas y vulnerabilidades para detectar los incidentes en la seguridad de la información. Se debieran considerar los siguientes lineamientos para los procedimientos de gestión de incidentes en la seguridad de la información:

- Se debieran establecer procedimientos para manejar los diferentes tipos de incidentes en la seguridad de la información, incluyendo:
  - Fallas del sistema de información y pérdida del servicio.
  - Código malicioso.
  - Negación del servicio.
  - Errores resultantes de data comercial incompleta o inexacta.
  - Violaciones de la confidencialidad e integridad.
  - Mal uso de los sistemas de información.
- Además de los planes de contingencia normales, los procedimientos también debieran cubrir:
  - Análisis e identificación de la causa del incidente.
  - Contención.
  - Planeación e implementación de la acción correctiva para evitar la recurrencia, si fuese necesario.

- Comunicaciones con aquellos afectados por o involucrados con la recuperación de un incidente.
- Reportar la acción a la autoridad apropiada.

- Se debiera recolectar y asegurar rastros de auditoría y evidencia similar, conforme sea apropiado para.
  - Análisis interno del problema.
  - Uso como evidencia forense en relación a una violación potencial del contrato o el requerimiento regulador o en el caso de una acción legal civil o criminal; por ejemplo, bajo la legislación sobre el mal uso de computadoras o protección de data.
  - Negociación para la compensación de los proveedores del software y servicio.
- Se debieran controlar formal y cuidadosamente las acciones para la recuperación de las violaciones de la seguridad y para corregir las fallas en el sistema; los procedimientos debieran asegurar que:
  - Sólo el personal claramente identificado y autorizado tengan acceso a los sistemas vivos y la data.
  - Se documenten en detalle todas las acciones de emergencia realizadas;
  - La acción de emergencia sea reportada a la gerencia y revisada de una manera adecuada.
  - La integridad de los sistemas y controles comerciales sea confirmada con una demora mínima.

Se debieran acordar con la gerencia los objetivos para la gestión de incidentes en la seguridad de la información, y se debieran asegurar que aquellos responsables de la gestión de incidentes en la seguridad de la información entiendan las prioridades de la organización para el manejo de los incidentes en la seguridad de la información.

Otra información

Los incidentes en la seguridad de la información podrían trascender fuera de las fronteras organizacionales y nacionales. Para responder a estos incidentes se necesita cada vez más coordinar la respuesta y compartir información sobre estos incidentes con organizaciones externas, conforme sea apropiado.

IV.9.8 *CONOCIMIENTO, EDUCACIÓN Y CAPACITACIÓN EN SEGURIDAD DE LA INFORMACIÓN (8.2.2)*

Control

Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceras personas debieran recibir una adecuada capacitación en seguridad y actualizaciones regulares sobre las políticas y procedimientos organizacionales conforme sea relevante para su función laboral.

Lineamiento de implementación

La capacitación y el conocimiento debieran comenzar con un proceso de inducción formal diseñado para introducir las políticas y expectativas de seguridad de la organización antes de otorgar acceso a la información o servicios.

La capacitación constante debiera incluir los requerimientos de seguridad, responsabilidades legales y controles comerciales, así como la capacitación en el uso correcto de los medios de procesamiento de información; por ejemplo, procedimiento de registro, uso de paquetes de software e información sobre los procesos disciplinarios.

Otra información

Las actividades de conocimiento, educación y capacitación debieran ser adecuados y relevantes para el rol, responsabilidades y capacidades de la persona, y debieran incluir información sobre amenazas conocidas, a quién contactar para mayor consultoría sobre seguridad y los canales apropiados para reportar los incidentes de seguridad de información.

La capacitación para aumentar la conciencia y conocimiento tiene como objetivo permitir a las personas reconocer los problemas e incidentes de la seguridad de la información, y responder de acuerdo a las necesidades de su rol en el trabajo.

IV.9.9 *PROTECCIÓN CONTRA EL CÓDIGO MALICIOSO Y MÓVIL (10.4)*

Objetivo:

Proteger la integridad del software y la integración.

Se requiere tomar precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no-autorizados.

El software y los medios de procesamiento de la información son vulnerables a la introducción de códigos maliciosos; como virus cómputo, virus de red, caballos Troyanos y bombas lógicas. Los usuarios debieran estar al tanto de los peligros de los códigos maliciosos. Cuando sea apropiado, los gerentes debieran introducir controles para evitar, detectar y eliminar los códigos maliciosos y controlar los códigos móviles.

IV.9.10 *CONTROLES CONTRA CÓDIGOS MALICIOSOS (10.4.1)*

Control

Controles de detección, prevención y recuperación para proteger contra códigos maliciosos y se debieran implementar procedimientos para el apropiado conocimiento del usuario.

Lineamiento de implementación

La protección contra códigos maliciosos se debiera basar en la detección de códigos maliciosos y la reparación de software, conciencia de seguridad, y los apropiados controles de acceso al sistema y gestión del cambio. Se debieran considerar los siguientes lineamientos:

- Establecer una política formal prohibiendo el uso de software no-autorizado.

- Establecer una política formal para proteger contra riesgos asociados con la obtención de archivos, ya sea a través de redes externas o cualquier otro medio, indicando las medidas de protección a tomarse.
- Realizar revisiones regulares del software y contenido de data de los sistemas que sostienen los procesos comerciales críticos; se debiera investigar formalmente la presencia de cualquier activo no-aprobado o enmiendas no-autorizadas.
- La instalación y actualización regular de software para la detección o reparación de códigos maliciosos para revisar las computadoras y medios como un control preventivo o una medida rutinaria; los chequeos llevados a cabo debieran incluir:
  - Chequeo de cualquier archivo en medios electrónicos u ópticos, y los archivos recibidos a través de la red para detectar códigos maliciosos antes de utilizarlo.
  - Chequear los adjuntos y descargas de los correos electrónicos para detectar códigos maliciosos antes de utilizarlos, este chequeo debiera llevarse a cabo en lugares diferentes; por ejemplo, servidores de correo electrónico, computadoras desktop y cuando se ingresa a la red de la organización.
  - Chequear las páginas Web para detectar códigos maliciosos.
- Definición, gestión, procedimientos y responsabilidades para lidiar con la protección de códigos maliciosos en los sistemas, capacitación en su uso, reporte y recuperación de ataques de códigos maliciosos.
- Preparar planes apropiados para la continuidad del negocio para recuperarse de ataques de códigos maliciosos, incluyendo toda la data y respaldo (back-up) de software y procesos de recuperación.
- Implementar procedimiento para la recolección regular de información, como suscribirse a listas de correos y/o chequear Web Sites que dan información sobre códigos maliciosos nuevos.

- Implementar procedimientos para verificar la información relacionada con el código malicioso y para asegurar que los boletines de advertencia sean exactos e informativos, los gerentes debieran asegurar que se utilicen fuentes calificadas; por ejemplo, periódicos acreditados, sitios de Internet confiables o proveedores que producen software para protegerse de códigos maliciosos; que diferencien entre bromas pesadas y códigos maliciosos reales; todos los usuarios debieran estar al tanto del problema de las bromas pesadas y qué hacer cuando se reciben.

Otra información

El uso de dos o más productos de software para protegerse de códigos maliciosos a través del ambiente de procesamiento de la información de diferentes vendedores puede mejorar la efectividad de la protección contra códigos maliciosos.

Se puede instalar software para protegerse de códigos maliciosos para proporcionar actualizaciones automáticas de archivos de definición y motores de lectura para asegurarse que la protección esté actualizada. Además, este software se puede instalar en cada desktop para que realice chequeos automáticos.

Se debiera tener cuidado de protegerse contra la introducción de códigos maliciosos durante el mantenimiento y procedimientos de emergencia, los cuales pueden evadir los controles de protección contra códigos maliciosos normales.

IV.9.11 *REPORTE DE LOS EVENTOS Y DEBILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN (13.1)*

Objetivo: Asegurar que los eventos y debilidades de la seguridad de la información asociados con los sistemas de información sean comunicados de una manera que permita que se realice una acción correctiva oportuna.

Se debieran establecer procedimientos formales de reporte y de la intensificación de un evento. Todos los usuarios empleados contratistas y terceros debieran estar al tanto de los procedimientos para el reporte de los diferentes tipos de eventos y debilidades que podrían tener un impacto en la seguridad de los activos

organizacionales. Se les debiera requerir que reporten cualquier evento y debilidad de la seguridad de la información lo más rápidamente posible en el punto de contacto designado

IV.9.12 *POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (5.1)*

Objetivo: Proporcionar a la gerencia la dirección y soporte para la seguridad de la información en concordancia con los requerimientos comerciales y las leyes y regulaciones relevantes.

La gerencia debiera establecer claramente la dirección de la política en línea con los objetivos comerciales y demostrar su apoyo, y su compromiso con, la seguridad de la información, a través de la emisión y mantenimiento de una política de seguridad de la información en toda la organización.

IV.9.13 *DOCUMENTO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (5.1.1)*

Control

El documento de la política de seguridad de la información debiera ser aprobado por la gerencia, y publicado y comunicado a todos los empleados y las partes externas relevantes.

Lineamiento de implementación

El documento de la política de seguridad de la información debiera enunciar el compromiso de la gerencia y establecer el enfoque de la organización para manejar la seguridad de la información. El documento de la política debiera contener enunciados relacionados con:

- Una definición de seguridad de la información, sus objetivos y alcance generales y la importancia de la seguridad como un mecanismo facilitador para intercambiar información (ver introducción).

- Un enunciado de la intención de la gerencia, fundamentando sus objetivos y los principios de la seguridad de la información en línea con la estrategia y los objetivos comerciales.
- Un marco referencial para establecer los objetivos de control y los controles, incluyendo la estructura de la evaluación del riesgo y la gestión de riesgo.
- Una explicación breve de las políticas, principios, estándares y requerimientos de conformidad de la seguridad de particular importancia para la organización, incluyendo.
    - Conformidad con los requerimientos legislativos, reguladores y restrictivos.
    - Educación, capacitación y conocimiento de seguridad.
    - Gestión de la continuidad del negocio.
    - Consecuencias de las violaciones de la política de seguridad de la información.
- Una definición de las responsabilidades generales y específicas para la gestión de la seguridad de la información incluyendo el reporte de incidentes de seguridad de la información.
- Referencias a la documentación que fundamenta la política; por ejemplo, políticas y procedimientos de seguridad más detallados para sistemas de información específicos o reglas de seguridad que los usuarios debieran observar.

Esta política de seguridad de la información se debiera comunicar a través de toda la organización a los usuarios en una forma que sea relevante, accesible y entendible para el lector objetivo.

Otra información

La política de seguridad de la información podría ser una parte del documento de política general. Si la política de seguridad de la información se distribuye fuera de la organización, se debiera tener cuidado de no divulgar información confidencial. Se puede encontrar mayor información en ISO/IEC 13335-1:2004.

IV.9.14 *CUMPLIMIENTO DE LOS REQUERIMIENTOS LEGALES (15.1)*

Objetivo

Evitar las violaciones a cualquier ley; regulación estatutaria, reguladora o contractual; y cualquier requerimiento de seguridad.

El diseño, operación, uso y gestión de los sistemas de información pueden estar sujetos a requerimientos de seguridad estatutarios, reguladores y contractuales.

Se debiera buscar la asesoría sobre los requerimientos legales específicos de los asesores legales de la organización o profesionales legales calificados adecuados. Los requerimientos legislativos varían de un país a otro y pueden variar para la información creada en un país que es transmitida a otro país (es decir, flujo de data inter-fronteras).

IV.9.15 *DERECHOS DE PROPIEDAD INTELECTUAL (15.1.2)*

Control

Se debieran implementar los procedimientos apropiados para asegurar el cumplimiento de los requerimientos legislativos, reguladores y contractuales sobre el uso del material con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentado.

Lineamiento de implementación

Se debieran considerar los siguientes lineamientos para proteger cualquier material que se considere de propiedad intelectual:

- Una política de cumplimiento de los derechos de propiedad intelectual y publicación que defina el uso legal de los productos de software e información.
- Sólo adquirir software a través de fuentes conocidos y acreditados para asegurar que no sean violados los derechos de autor.
- Mantener el conocimiento de las políticas para proteger los derechos de propiedad intelectual, y notificar de la voluntad de tomar una acción disciplinaria contra el personal que los viole.
- Monitorear los registros de activos apropiados, e identificar todos los activos con los requerimientos para proteger los derechos de propiedad intelectual.
- Mantener prueba y evidencia de la propiedad de las licencias, discos maestros, manuales, etc.
- Implementar controles para asegurar que no se exceda el número máximo de usuarios permitidos.
- Llevar a cabo chequeos para que sólo se instalen software autorizados y productos con licencia.
- Proporcionar una política para mantener las condiciones de licencias apropiadas.
- Proporcionar una política para eliminar o transferir el software a otros.
- Utilizar las herramientas de auditoría apropiadas.
- Cumplir con los términos y condiciones del software e información obtenida de redes públicas.
- No duplicar, convertir a otro formato o extraer de registros comerciales (audio, vídeo), aparte de los permitidos por la ley de derechos de autor.
- No copiar; completamente o en parte; libros, artículos, reportes u otros documentos; aparte de aquellos permitidos por la ley de derechos de autor.

Otra información

Los derechos de propiedad intelectual incluyen los derechos de autor, derechos de diseño, marcas registradas, patentes y licencias de código fuente de software o documentos.

Los productos de software patentados usualmente son suministrados mediante un contrato de licencia que especifica los términos y condiciones de las licencias, por ejemplo, limitando el uso de los productos a máquinas específicas o limitando el copiado sólo a la creación de copias de respaldo. Se necesita aclarar la situación IPR del software desarrollado por la organización con el personal.

Los requerimientos legislativos, reguladores y contractuales pueden colocar restricciones sobre el copiado de material patentado. En particular, ellos pueden requerir que sólo se pueda utilizar el material desarrollado por la organización, o que sea licenciado o provisto por un diseñador a la organización. La violación de los derechos de autor puede llevar a una acción legal, lo cual puede involucrar los trámites judiciales.

IV.9.16 *PROTECCIÓN DE LA DATA Y PRIVACIDAD DE LA INFORMACIÓN PERSONAL (15.1.4)*

Control

Se debiera asegurar la protección y privacidad de la data conforme lo requiera la legislación, regulaciones y, si fuesen aplicables, las cláusulas contractuales relevantes.

Lineamiento de implementación

Se debiera desarrollar e implementar una política de protección y privacidad de la data. Esta política debiera ser comunicada a todas las personas involucradas en el procesamiento de la información personal.

El cumplimiento de esta política y toda legislación y regulación de protección de data relevante requiere una apropiada estructura y control gerencial. Con frecuencia esto se logra asignando a una persona como responsable, por ejemplo un funcionario de

protección de data, quien debiera proporcionar lineamientos a los gerentes, usuarios y proveedores de los servicios sobre sus responsabilidades individuales y los procedimientos específicos que debieran seguir.

La responsabilidad por el manejo de la información personal y el reforzamiento del conocimiento de los principios de protección de data debieran ser tratados en concordancia con la legislación y las regulaciones relevantes. Se debieran implementar las apropiadas medidas técnicas y organizacionales para protección la información personal.

Otra información

Un número de países han introducido una legislación colocando controles sobre la recolección, procesamiento y transmisión de data personal (generalmente la información sobre personas vivas que pueden ser identificadas mediante esa información). Dependiendo de la legislación nacional respectiva, dichos controles pueden imponer impuestos a aquellos que recolectan, procesan y difunden información personal; y pueden restringir la capacidad para transferir la data a otros países.

IV.9.17 *RESPONSABILIDAD POR LOS ACTIVOS (7.1)*

Objetivo

Lograr y mantener una apropiada protección de los activos organizacionales.

Todos los activos debieran ser inventariados y contar con un propietario nombrado.

Los propietarios debieran identificar todos los activos y se debiera asignar la responsabilidad por el mantenimiento de los controles apropiados. La implementación de controles específicos puede ser delegada por el propietario conforme sea apropiado, pero el propietario sigue siendo responsable por la protección apropiada de los activos.

IV.9.18 INVENTARIO DE LOS ACTIVOS (7.1.1)

Control

Se debieran identificar todos los activos y se debiera elaborar y mantener un inventario de todos los activos importantes.

Lineamiento de implementación

Una organización debiera identificar todos los activos y documentar la importancia de estos activos. El inventario de los activos debiera incluir toda la información necesaria para poder recuperarse de un desastre; incluyendo el tipo de activo, formato, ubicación, información de respaldo, información de licencias y un valor comercial. El inventario no debiera duplicar innecesariamente otros inventarios, pero se debiera asegurar que el contenido esté alineado.

Además, se debiera acordar y documentar la propiedad y la clasificación de la propiedad para cada uno de los activos. Basados en la importancia del activo, su valor comercial y su clasificación de seguridad, se debieran identificar los niveles de protección que se conmensuran con la importancia de los.

Otra información

Existen muchos tipos de activos, incluyendo:

- Información: bases de datos y archivos de data, contratos y acuerdos, documentación del sistema, información de investigaciones, manuales del usuario, material de capacitación, procedimientos operacionales o de soporte, planes de continuidad del negocio, acuerdos para contingencias, rastros de auditoría e información archivada.
- Activos de software: software de aplicación, software del sistema, herramientas de desarrollo y utilidades.
- Activos físicos: equipo de cómputo, equipo de comunicación, medios removibles y otro equipo.

- Servicios: servicios de computación y comunicación, servicios generales; por ejemplo, calefacción, iluminación, energía y aire acondicionado.
- Personas, y sus calificaciones, capacidades y experiencia.
- Intangibles, tales como la reputación y la imagen de la organización.

Los inventarios de los activos ayudan a asegurar que se realice una protección efectiva de los activos, y también puede requerir de otros propósitos comerciales; como planes de salud y seguridad, seguros o razones financieras (gestión de activos). El proceso de compilar un inventario de activos es un pre-requisito importante de la gestión del riesgo.

IV.9.19 *PROPIEDAD DE LOS ACTIVOS (7.1.2)*

Control

Toda la información y los activos asociados con los medios de procesamiento de información debieran ser propiedad de una parte designada de la organización.

Lineamiento de implementación

El propietario del activo debiera ser responsable de:

- Asegurar que la información y los activos asociados con los medios de procesamiento de la información sean clasificados apropiadamente.
- Definir y revisar periódicamente las restricciones y clasificaciones de acceso, tomando en cuenta las políticas de control de acceso aplicables.
- La propiedad puede ser asignada a:
- Un proceso comercial.
- Un conjunto de actividades definido.
- Una aplicación.
- Un conjunto de data definido.

Otra información

Se pueden delegar las tareas rutinarias; por ejemplo, a un custodio que supervisa el activo diariamente, pero la responsabilidad permanece con el propietario.

En los sistemas de información complejos podría ser útil designar grupos de activos, los cuales actúan juntos para proporcionar una función particular como "servicios". En este caso el propietario es responsable de la entrega del servicio, incluyendo el funcionamiento de los activos que los proveen.

IV.9.20 *USO ACEPTABLE DE LOS ACTIVOS (7.1.3)*

Control

Se debieran identificar, documentar e implementar reglas para el uso aceptable de la información y los activos asociados con los medios del procesamiento de la información.

Lineamiento de implementación

Todos los empleados, contratistas y terceros debieran seguir las reglas para el uso aceptable de la información y los activos asociados con los medios del procesamiento de la información, incluyendo:

- Reglas para la utilización del correo electrónico e Internet.
- Lineamientos para el uso de dispositivos móviles, especialmente para el uso fuera del local de la organización.

La gerencia relevante debiera proporcionar reglas o lineamientos específicos. Los empleados, contratistas y terceros que usan o tienen acceso a los activos de la organización debieran estar al tanto de los límites existentes para su uso de la información y los activos asociados con los medios y recursos del procesamiento de la información de la organización. Ellos debieran ser responsables por el uso que le den a cualquier recurso de procesamiento de información, y de cualquier uso realizado bajo su responsabilidad.

IV.9.21 CLASIFICACIÓN DE LA INFORMACIÓN (7.2)

Objetivo

Asegurar que la información reciba un nivel de protección apropiado.

La información debiera ser clasificada para indicar la necesidad, prioridades y grado de protección esperado cuando se maneja la información.

La información tiene diversos grados de confidencialidad e importancia. Algunos ítems pueden requerir un nivel de protección adicional o manejo especial. Se debiera utilizar un esquema de clasificación de información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas de uso especiales

IV.9.22 LINEAMIENTOS DE CLASIFICACIÓN (7.2.1)

Control

Se debiera clasificar la información en términos de su valor, requerimientos legales, sensibilidad y grado crítico para la organización.

Lineamiento de implementación

Las clasificaciones y los controles de protección asociados para la información debieran tomar en cuenta las necesidades comerciales de intercambiar o restringir información y los impactos comerciales asociados con dichas necesidades.

Los lineamientos de clasificación debieran incluir protocolos para la clasificación inicial y la reclasificación a lo largo del tiempo; en concordancia con alguna política pre-determinada de control de acceso.

Debiera ser responsabilidad del propietario del activo definir la clasificación de un activo, revisarla periódicamente y asegurarse que se mantenga actualizada y en el nivel apropiado.

Se debiera tener en consideración el número de categorías de clasificación y los beneficios a obtenerse con su uso.

Los esquemas demasiado complejos pueden volverse engorrosos y anti-económicos de utilizar o pueden volverse poco prácticos. Se debiera tener cuidado al interpretar los encabezados de la clasificación en los documentos de otras organizaciones, los cuales pueden tener definiciones diferentes para encabezados con el mismo nombre o nombre similares.

Otra información

Se puede evaluar el nivel de protección analizando la confidencialidad, integridad y disponibilidad, y cualquier otro requerimiento para la información considerada.

Con frecuencia, la información deja de ser sensible o crítica después de cierto período de tiempo, por ejemplo, cuando la información se ha hecho pública. Se debieran tomar en cuenta estos aspectos, ya que la sobre-clasificación puede llevar a la implementación de controles innecesarios resultando en un gasto adicional.

Agrupar documentos con requerimientos de seguridad similares cuando se asignan niveles de clasificación podría ayudar a simplificar la tarea de clasificación.

En general, la clasificación dada a la información es una manera rápida para determinar cómo se está manejando y protegiendo la información.

IV.9.23 *ETIQUETADO Y MANEJO DE LA INFORMACIÓN (7.2.2)*

Control

Se debiera desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado y manejo de la información en concordancia con el esquema de clasificación adoptado por la organización.

Lineamiento de implementación

Los procedimientos para el etiquetado de la información necesitan abarcar los activos de información en formatos físicos y electrónicos. El output de los sistemas conteniendo información que es clasificada como sensible o crítica debiera llevar la etiqueta de clasificación apropiada (en el output). El etiquetado debiera reflejar la clasificación de acuerdo a las reglas establecidas en 7.2.1. Los ítems a considerarse

incluyen reportes impresos, presentaciones en pantalla, medios de grabación (por ejemplo; cintas, discos, CDs), mensajes electrónicos y transferencia de archivos.

Para cada nivel de clasificación, se debiera definir los procedimientos de manejo seguros; incluyendo el procesamiento, almacenaje, transmisión, de-clasificación y destrucción. Esto también debiera incluir los procedimientos de la cadena de custodia y el registro de cualquier incidente de seguridad relevante.

Los acuerdos con otras organizaciones que incluyen intercambio de información debieran incluir procedimientos para identificar la clasificación de esa información e interpretar las etiquetas de clasificación de otras organizaciones.

Otra información

El etiquetado y el manejo seguro de la información clasificada es un requerimiento clave para los acuerdos de intercambio de información. Las etiquetas físicas son una forma común de etiquetado. Sin embargo, algunos archivos de información, como documentos en forma electrónica, no pueden ser etiquetados físicamente y se necesitan medios electrónicos para el etiquetado. Por ejemplo, la etiqueta de notificación puede aparecer en la pantalla. Cuando no es factible el etiquetado, se pueden aplicar otros medios para designar la clasificación de la información; por ejemplo, mediante procedimientos o meta-data.

IV.10 TIPOS DE AMENAZAS

Se presenta a continuación un catálogo de amenazas posibles sobre los activos de un sistema de información:

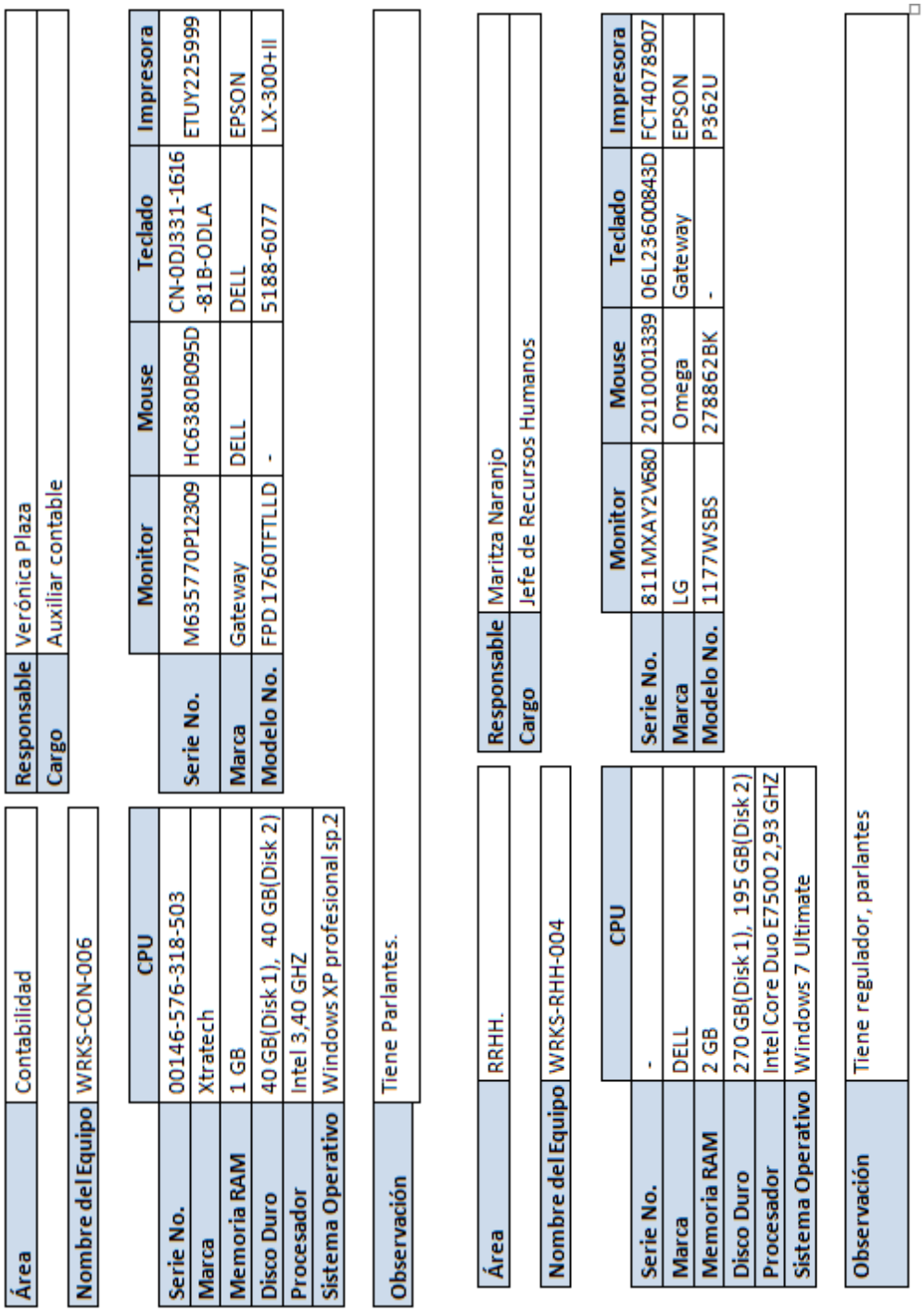
AMENAZAS SOBRE LOS ACTIVOS HARDWARE / SOFTWARE (APLICACIONES/DATOS/INFORMACIÓN)		
DESASTRES NATURALES [N]		
Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.		
[N.1]	**Incendios**	Posibilidad de que el fuego destruya o dañe el activo.
[N.2]	**Inundaciones**	Posibilidad de que el agua Destruya o dañe el activo.
[N.3]	**Otro desastre natural**	Posibilidad de que otros incidentes tales como: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, etc. destruyan o dañen el activo.
DE ORIGEN INDUSTRIAL [I]		
Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.		
[I.1]	**Incendio**	Posibilidad de que el fuego acabe con los recursos del sistema.
[I.2]	**Escapes, fugas, inundaciones**	Posibilidad de que el agua acabe con los recursos del sistema.
[I.3]	**Contaminación mecánica**	Vibraciones, polvo, suciedad.
[I.4]	**Avería de origen físico**	Fallos en los equipos. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema. Las consecuencias que se derivan, esta distinción no suele ser relevante.
[I.5]	**Corte del suministro eléctrico**	Cese de la alimentación de potencia.
[I.6]	**Condiciones inadecuadas de temperatura y/o humedad**	Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad.
ERRORES Y FALLOS NO INTENCIONADOS [E]		
Fallos no intencionales causados por las personas.		
[E.1]	**Errores del administrador**	Equivocaciones de personas con responsabilidades de instalación y operación.
[E.2]	**Errores de los usuarios**	Equivocaciones de las personas cuando usan los servicios, datos, etc.
[E.3]	**Errores de monitorización (log)**	Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados.
[E.4]	**Errores de configuración**	Introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.
[E.5]	**Difusión de software dañino**	Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.

[E.7]	**Escapes de información**	La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.
[E.8]	**Alteración de la información**	Alteración accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
[E.9]	**Introducción de información incorrecta**	Inserción accidental de información incorrecta. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
[E.10]	**Degradación de la información**	Degradación accidental de la información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
[E.11]	**Destrucción de información**	Pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
[E.12]	**Divulgación de información**	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc.
[E.13]	**Vulnerabilidades de los programas (software)**	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.
[E.14]	**Errores de mantenimiento / actualización de programas (software)**	Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.
[E.15]	**Errores de mantenimiento / actualización de equipos (hardware)**	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.
[E.16]	**Caída del sistema por agotamiento de recursos**	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
ATAQUES INTENCIONADOS [A]		
Fallos deliberados causados por las personas.		
[A.1]	**Manipulación de la configuración**	Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.
[A.2]	**Suplantación de la identidad del usuario**	Cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.
[A.3]	**Abuso de privilegios de acceso**	Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.
[A.4]	**Uso no previsto**	Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales, etc.

[A.5]	**Difusión de software dañino**	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.
[A.7]	**Acceso no autorizado**	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente.
[A.10]	**Modificación de la información**	Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
[A.11]	**Introducción de falsa información**	Inserción interesada de información falsa, con ánimo de obtener un beneficio o causar un perjuicio. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
[A.12]	**Corrupción de la información**	Degradación intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
[A.13]	**Destrucción la información**	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.
[A.14]	**Divulgación de información**	Revelación de información.
[A.15]	**Manipulación de programas**	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.
[A.16]	**Denegación de servicio**	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.
[A.17]	**Robo**	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal.
[A.18]	**Ataque destructivo**	Vandalismo, terrorismo, acción militar. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.
[A.19]	**Ocupación enemiga**	Cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.

Tabla 18 - Amenaza sobre los activos Hardware, Software, Información

IV.11 INVENTARIO GENERAL DE PLASTICOS INTERNACIONALES C.A



Área	Contabilidad
Nombre del Equipo	WRKS-CON-006

Responsable	Verónica Plaza
Cargo	Auxiliar contable

CPU		Monitor	Mouse	Teclado	Impresora
Serie No.	00146-576-318-503	M635770P12309	HC63808095D	CN-0DJ331-1616 -81B-ODLA	ETUY225999
Marca	Xtratech	Gateway	DELL	DELL	EPSON
Memoria RAM	1 GB	Gateway	DELL	DELL	EPSON
Disco Duro	40 GB(Disk 1), 40 GB(Disk 2)	FPD1760TFTLLD	-	5188-6077	LX-300+II
Procesador	Intel 3,40 GHZ				
Sistema Operativo	Windows XP profesional sp2				

Observación	Tiene Parlantes.

Área	RRHH.
Nombre del Equipo	WRKS-RHH-004

Responsable	Maritza Naranjo
Cargo	Jefe de Recursos Humanos

CPU		Monitor	Mouse	Teclado	Impresora
Serie No.	-	811MXAY2W680	2010001339	06L23600843D	FCT4078907
Marca	DELL	LG	Omega	Gateway	EPSON
Memoria RAM	2 GB	1177WSBS	278862BK	-	P362U
Disco Duro	270 GB(Disk 1), 195 GB(Disk 2)				
Procesador	Intel Core Duo E7500 2,93 GHZ				
Sistema Operativo	Windows 7 Ultimate				

Observación	Tiene regulador, parlantes

Área	Sistemas

Responsable	José Rivera
Cargo	Jefe de Sistemas

Nombre del Equipo	WRKS-SIS-023

SERVIDOR 1	
Memoria RAM	2 GB
Disco Duro	80 GB (Disk 1) 80 GB (Disk 2)
Procesador	XEON 3,00 GHZ
Sistema Operativo	Windows Server 2003 sp.1

	Monitor	**Mouse**	**Teclado**	**Impresora**
Serie No.	MlR7150N 18341	X65130404997	15100500735	-
Marca	Gateway	Genius	Omega	-
Modelo No.	-	278862BK	-	-

Nombre del Equipo	WRKS-SIS-022

Nombre del Equipo	WRKS-SIS-023

SERVIDOR 2	
Memoria RAM	16 GB
Disco Duro	300 GB
Disco Externo	500 GB
Procesador	XEON 3,00 GHZ
Sistema Operativo	Windows Server 2008 SP.1

Área	Producción
Nombre del Equipo	WRKS-PRO-011

Responsable	Jaime Rodríguez
Cargo	Asistente de Producción

CPU	
Serie No.	-
Marca	DELL
Memoria RAM	2 GB
Disco Duro	160 GB
Procesador	Intel Pentium Dual Core 2.00GHz
Sistema Operativo	Windows 7 (32 bits)

Monitor		Mouse		Teclado		Impresora	
Serie No.	-			-		G8DY319861	
Marca	LG		DELL			EPSON	
Modelo No.	Flatron L177WSB			-		LX-300+II	

Observación	Tiene Parlantes.

Área	Recepción
Nombre del Equipo	WRKS-REC-001

Responsable	Jennifer Rodríguez
Cargo	Auxiliar de Crédito

CPU	
Serie No.	-
Marca	Omega
Memoria RAM	1 GB
Disco Duro	292 GB (Disk 1), 187 GB (Disk 2)
Procesador	Core 2 Duo
Sistema Operativo	Windows 7 Ultimate

Monitor		Mouse		Teclado		Impresora	
Serie No.	-		-		-		-
Marca	Samsung	Genius		BenQ		-	
Modelo No.	-		-		-		-

Observación	-

Área	Producción
Nombre del Equipo	WRKS-PRO-013

CPU	
Serie No.	-
Marca	DELL
Memoria RAM	2 GB
Disco Duro	160 GB
Procesador	Intel Pentium Dual Core 2.00GHz
Sistema Operativo	Windows Vista Home Basic SP1

Responsable	Silvana Quinde
Cargo	Asistente de Producción

Monitor	Mouse	Teclado	Impresora
--	H17039XY	-	-
Acer	DELL	DELL	-
X153W	OXN967	SK-8165	-

Observación	-

Área	Salón de Presentaciones
Nombre del Equipo	WRKS-PRE-003

CPU	
Serie No.	-
Marca	Xtratech
Memoria RAM	-
Disco Duro	-
Procesador	-
Sistema Operativo	-

Responsable	-
Cargo	-

Monitor	Mouse	Teclado	Impresora
143BM28HC675	-	1510003004111	-
Compaq	-	Omega	-
v570	-	-	-

Observación	Monitor, teclado y CPU en el piso.

Área	Sellado
Nombre del Equipo	WRKS-SEL-014

Responsable	Víctor Cevallos
Cargo	Jefe de Área

CPU	Monitor	Mouse	Teclado	Impresora
Serie No.	-	-	-	-
Marca	Compaq	Compaq	Compaq	EPSON
Modelo No.	MV540			LX300+II
Memoria RAM	256 MB			
Disco Duro	40 GB			
Procesador	Intel Pentium 4 1.6 GHz			
Sistema Operativo	XP Home Edition			

Observación	Tienen Balanza electrónica Marca: CAS, Modelo: CI-2001AS. Otra Impresora Zebra TLP2844.

Área	Impresión
Nombre del Equipo	WRKS-IMP-15

Responsable	Enrique Valle
Cargo	Gerente Técnico

CPU	Monitor	Mouse	Teclado	Impresora
Serie No.	-	-	-	08C074000645
Marca	ViewSonic	-	Compaq	Zebra
Modelo No.	PF775B	-	-	ZM400
Marca	Clon			
Memoria RAM	768 MB			
Disco Duro	-			
Procesador	Intel Pentium IV 2.40 GHZ			
Sistema Operativo	Windows XP SP3			

Observación	-

Área	Bodega

Responsable	Carlos Bailón
Cargo	Jefe de Bodega

Nombre del Equipo	WRKS-BOD-019

CPU	
Serie No.	79PLHKI
Marca	DELL
Memoria RAM	2 GB
Disco Duro	
Procesador	AMD Athlon x2 Dual Core 1.5 GHz
Sistema Operativo	Windows 7 Profesional

Monitor	Mouse	Teclado	Impresora
146BA46TD035	-	-	-
Compaq	DELL	DELL	EPSON
MB540	XN966		LX300+II

Observación	CPU Compacto. Impresora compartida.

Área	EXTRUSIÓN

Responsable	-
Cargo	-

Nombre del Equipo	WRKS-EXT-016

CPU	
Serie No.	
Marca	Compaq
Memoria RAM	256 MB
Disco Duro	
Procesador	Pentium IV 1.5GHZ
Sistema Operativo	Windows XP Profesional SP2

Monitor	Mouse	Teclado	Impresora
-	-	-	-
Proview	DELL	Anti-RSI	EPSON
-			LX300+

Observación	Otra Impresora Zebra TLP2844. Balanza electrónica CAS CI2002001A.

Área	Calidad
Nombre del Equipo	WRKS-CAL-017

CPU	
Serie No.	
Marca	
Memoria RAM	2 GB
Disco Duro	96.6 GB (Disk 1) 135 GB (Disk 2)
Procesador	Intel Athlon 3.6 GHz
Sistema Operativo	Vista Ultimate

Observación	-

Responsable	María Del Carmen
Cargo	Asistente de Calidad

	Monitor	Mouse	Teclado	Impresora
Serie No.	-	-	-	-
Marca	-	-	TECH	EPSON
Modelo No.	-	-	-	TX300F

Área	Bodega
Nombre del Equipo	WRKS-BOD-020

CPU	
Serie No.	-
Marca	-
Memoria RAM	1 GB
Disco Duro	512 GB
Procesador	Intel Core2Duo 2.93GHz
Sistema Operativo	Windows 7

Observación	-

Responsable	José Bravo
Cargo	Asistente de Bodega

	Monitor	Mouse	Teclado	Impresora
Serie No.	ETMSA004407026	-	-	-
Marca	BenQ	-	BenQ	-
Modelo No.	-	-	KB-28G	-

Área	Producción
Nombre del Equipo	WRKS-PRO-009

CPU	
Serie No.	XCX7121004204
Marca	Gateway
Memoria RAM	2 GB
Disco Duro	160 GB
Procesador	Athlon Dual Core 2.6 GHz
Sistema Operativo	Windows 7 Ultimate

Responsable	Carlos Stagg
Cargo	Asistente de Cobranzas

	Monitor	Mouse	Teclado	Impresora
Serie No.	-	-	-	-
Marca	-	-	Omega	-
Modelo No.	-	-	-	-

Observación	-

Área	Calidad
Nombre del Equipo	-

CPU	
Serie No.	-
Marca	-
Memoria RAM	1GB
Disco Duro	-
Procesador	Intel Core2Duo 2.93GHz
Sistema Operativo	Windows 7 profesional

Responsable	-
Cargo	-

	Monitor	Mouse	Teclado	Impresora
Serie No.	-	-	-	-
Marca	-	-	Markvision	-
Modelo No.	-	-	-	-

Observación	

Área	Producción
Nombre del Equipo	WRKS-PRO-008

Responsable	Silvia Sarmiento
Cargo	Jefa de Cobranzas

CPU	
Serie No.	-
Marca	HP Compaq
Memoria RAM	1 GB
Disco Duro	-
Procesador	Intel Pentium IV 3GHz
Sistema Operativo	Windows XP Profesional SP2

Monitor	Mouse	Teclado	Impresora
-	-	-	-
Compaq	-	-	EPSON
-	-	-	LX300+II

Serie No.	
Marca	
Modelo No.	

Observación
Otra Impresora EPSON EX-2190.

Área	Recepción
Nombre del Equipo	WRKS-REC-002

Responsable	Mabel Arévalo
Cargo	Auxiliar de crédito

CPU	
Serie No.	-
Marca	Omega
Memoria RAM	1 GB
Disco Duro	232 GB
Procesador	Athlon 1.6GHz
Sistema Operativo	Windows XP SP3

Monitor	Mouse	Teclado	Impresora
-	-	-	-
Dell	Genius	HP	EPSON
E178FPV	-	-	LX300+II

Serie No.	
Marca	
Modelo No.	

Observación
-

Área	Producción
Nombre del Equipo	WRKS-PRO-012

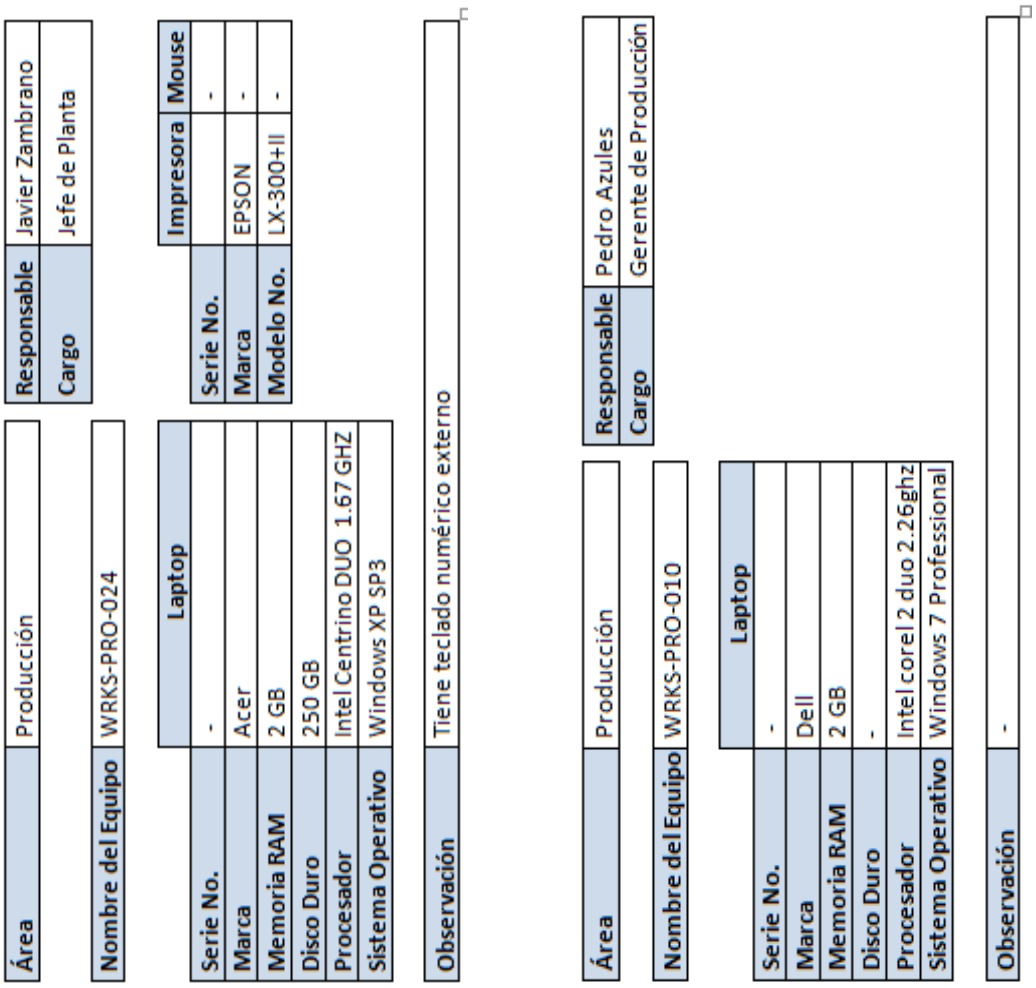
Responsable	Luis Valle
Cargo	Asistente de producción

CPU	
Serie No.	D945GCLF2D
Marca	Intel
Memoria RAM	1 GB
Disco Duro	225 GB (Disk 1), 8 GB (Disk 2)
Procesador	Intel 1.60 GHZ
Sistema Operativo	Windows XP Profesional sp.3

	Monitor	**Mouse**	**Teclado**	**Impresora**
Serie No.	-	64784200467	BE72603954	LX-300+II
Marca	DELL	Genius	HP	EPSON
Modelo No.	E178Fpv	NetScroll 120	-	68D4154202

Observación	Tiene regulador, parlantes

EQUIPOS MÓVILES



Área	Producción
Nombre del Equipo	WRKS-PRO-024

Responsable	Javier Zambrano
Cargo	Jefe de Planta

Laptop		Impresora	Mouse
Serie No.	-	Serie No.	-
Marca	Acer	Marca	EPSON	-
Memoria RAM	2 GB	Modelo No.	LX-300+II	-
Disco Duro	250 GB			
Procesador	Intel Centrino DUO 1.67 GHZ			
Sistema Operativo	Windows XP SP3			

Observación	Tiene teclado numérico externo

Área	Producción
Nombre del Equipo	WRKS-PRO-010

Responsable	Pedro Azules
Cargo	Gerente de Producción

Laptop	
Serie No.	-
Marca	Dell
Memoria RAM	2 GB
Disco Duro	-
Procesador	Intel corel 2 duo 2.26ghz
Sistema Operativo	Windows 7 Professional

Observación	-

Área	Calidad
Nombre del Equipo	WRKS-CAL-018

Laptop	
Serie No.	00144-187-857-238
Marca	HP Compaq
Memoria RAM	1 GB
Disco Duro	-
Procesador	Intel Dual Core 1.46 GHz
Sistema Operativo	Windows XP Profesional SP3

Responsable	Andrés Cepeda
Cargo	Jefe de Calidad

	Impresora	Mouse
Serie No.	-	-
Marca	-	-
Modelo No.	-	-

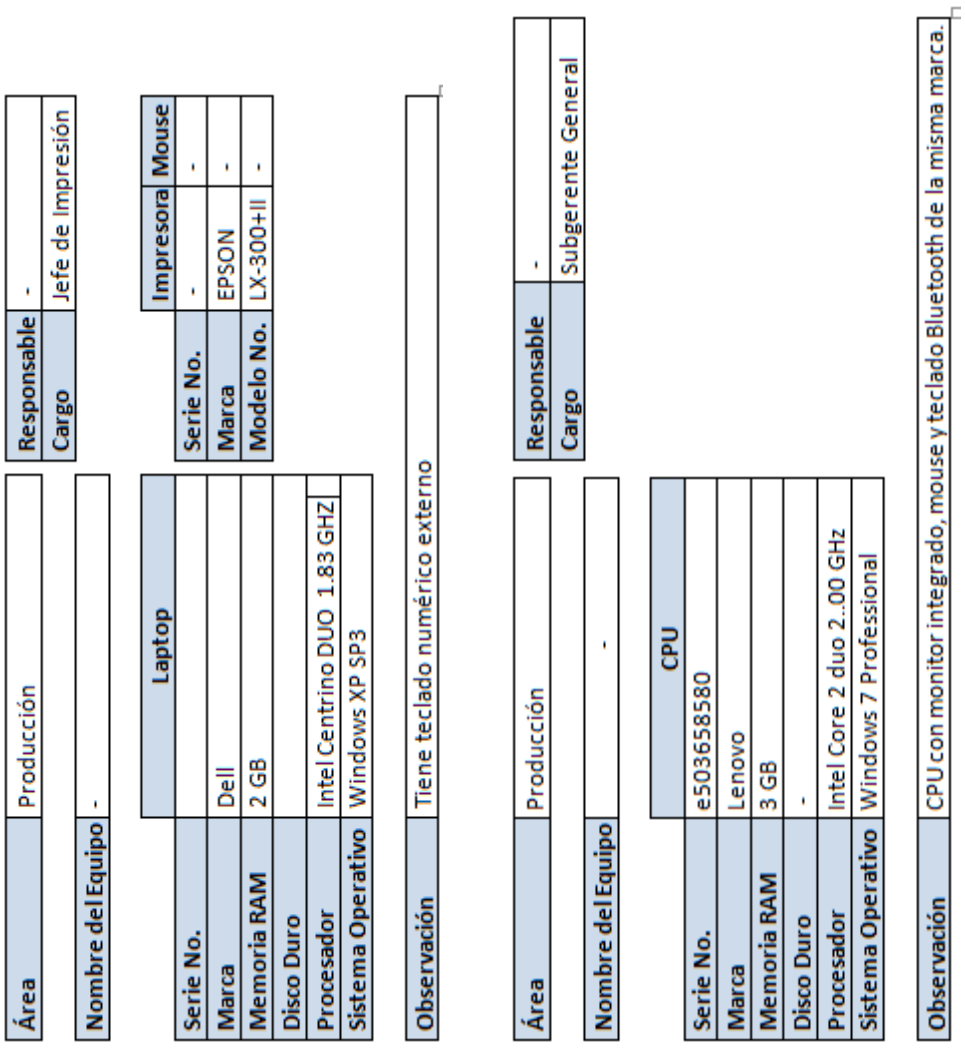
Observación	Impresora compartida a María del Carmen.

Área	Bodega
Nombre del Equipo	-

Responsable	-
Cargo	-

Recolector	
Serie No.	-
Marca	Motorola
Memoria RAM	40 MB
Disco Duro	
Procesador	Intel TXA 207
Sistema Operativo	Windows Compact Edition 5.0

Observación	-



Área	Producción
Nombre del Equipo	-

Responsable	-
Cargo	Jefe de Impresión

Laptop	
Serie No.	
Marca	Dell
Memoria RAM	2 GB
Disco Duro	
Procesador	Intel Centrino DUO 1.83 GHZ
Sistema Operativo	Windows XP SP3

Impresora	Mouse
-	-
EPSON	-
LX-300+II	-

Serie No.	
Marca	
Modelo No.	

Observación
Tiene teclado numérico externo

Área	Producción
Nombre del Equipo	-

Responsable	-
Cargo	Subgerente General

CPU	
Serie No.	e503658580
Marca	Lenovo
Memoria RAM	3 GB
Disco Duro	-
Procesador	Intel Core 2 duo 2..00 GHz
Sistema Operativo	Windows 7 Professional

Observación	CPU con monitor integrado, mouse y teclado Bluetooth de la misma marca.

Tabla 19 - Inventario de activos

IV.12 FOTOS DE LA EMPRESA

Figura - 5 La empresa

IV.13 DIFERENTES INSTALACIONES DE LA EMPRESA

Figura - 6 Área de Computación

Figura - 7 Área de Producción

Figura - 8 Área de Asistente de Producción

Figura - 9 Área de Producción

Figura - 10 Área de Producción

Figura - 11 Área de Contabilidad

Figura - 12 Área de Contabilidad

Figura - 13 Área de Contabilidad

Figura - 14 Recepción 1

Figura - 15 Recepción 2

Figura - 16 Bodega 1

Figura - 17 Área de Extrusión

Figura - 18 Impresión

Figura - 19 Sellado

IV.14 DIFERENTES PROBLEMAS ENCONTRADOS EN LA EMPRESA CON RESPECTO A LA SEGURIDAD INFORMÁTICA

Figura - 20 Diferentes Problemas Encontrados