UNIVERSIDAD EMPRESARIAL SIGLO 21

Trabajo final de graduación,
Licenciatura en Informática.

"Seguridad Informática en la planta industrial de ARCOR en Colonia Caroya."

Alumno: Guillermo Young Barbé

Legajo: INF 141

Tutor: Enzo Daniel García

Julio de 2005

Índice.

Índice. 3

Introducción: 6

Antecedentes: 7

Descripción general sobre la problemática: 7

Formulación del problema: 9

Justificación: 9

Descripción de la Organización: 10

Objetivo: 12

Alcances del trabajo: 12

Limites: 12

Marco Teórico. 13

¿Qué es la información y cuáles son sus atributos? 13

Uno de los atributos de la información: la SEGURIDAD. 14

¿Qué se requiere para proveer de una seguridad efectiva? 15

Aspectos de Seguridad Informática: 18

Mapa de Seguridad 21

Análisis de riesgo: 23

¿De quién debemos protegernos? 23

¿Qué se debe proteger? 24

¿Contra qué debe protegerse? 24

Secuencia de un ataque. 25

Relación Operatividad–Seguridad 28

Métodos y guías de análisis sobre seguridad informática. 31

Guías MAGERIT 31

Metodología de trabajo: 33

Relevamiento 35

Información sobre la Planta Industrial 35

Evaluación (descriptiva) de la situación. 53

Seguridad física: 53

Mantenimiento de equipos. Contratos con proveedores de servicio: 57

Seguridad del equipamiento fuera del ámbito de la empresa: 58

Baja segura o reutilización de equipamiento: Licencias. Datos: 58

Ingeniería social: 58

Políticas y Procedimientos: 59

Plan de contingencias: 60

Seguridad de Servidores y Estaciones de Trabajo: 60

Procedimientos de configuraciones de seguridad en servidores: 60

Utilización de la red y recursos compartidos: 61

Correo electrónico: 61

Antivirus: 62
Backups: 62

Identificación de Activos 64
1. Activos relacionados con el nivel del Entorno. 64
2. Activos relacionados con el nivel de los Sistemas de Información. 66
3. Activos relacionados con el nivel de la Información. 68
4. Activos relacionados con el nivel de las Funcionalidades de la organización. 70
5. Otros Activos no relacionados con los niveles anteriores. 70

Interpretación y análisis de la información recolectada. 72
Resumen gráfico de la valoración de riesgos de activos. 88
Conclusión sobre el análisis de riesgos de activos identificados: 90
Conclusión sobre encuestas - preguntas abiertas: 91
Conclusión sobre encuestas - preguntas cerradas: 92

Propuesta 94

Esquema de la metodología seguida. 95

Activos seleccionados. 96

Propuesta de políticas de Seguridad Informática. 97

Política de Seguridad informática - ARCOR SAIC – Div. Chocolates. 100
Justificación: 100
Responsabilidades: 101
Política de Uso aceptable de equipos informáticos. 103
Política de contraseñas 107
Política de seguridad en Servidores 111
Política de Anti-virus 114
Política de uso del correo electrónico 115
Política de encriptación aceptable 116
Política de comunicaciones inalámbricas 117

Aplicación de controles acordes a la norma IRAM-ISO 17799 119
1 - Controles aplicados sobre equipos de computación en general: 120
2 - Controles sobre equipos móviles: 123
3 - Controles aplicados sobre equipos de Radio Frecuencia: 125
4 - Controles aplicados sobre el servidor de Programación de Producción: 129
5 - Controles aplicados sobre servidores de archivo: 130
6 - Controles aplicados en el Centro de Cómputos (Seg. Física): 133

Procedimientos. 134
Procedimiento para la configuración de seguridad en equipos de escritorio o móviles. 134
Procedimiento de configuración de Access Points y Unidades Móviles. 137
Procedimiento de configuración de seguridad de un Servidor Windows 2000. 142
Procedimientos recomendados para Anti-virus 152

Planes de contingencia. 153
Plan de contingencia ante extravío, robo o rotura de equipos móviles críticos. 153
Plan de contingencia ante desperfectos en equipos de la red inalámbrica. 154

Conclusión. 155

Anexo 1 (Política del Sistema de Gestión Integral – S.G.I.) 157

Anexo 2 (Replicación de seguridad en redes inalámbricas) ____ *159*

Anexo 3 (Encuesta a usuarios – consolidación.) ____ *164*

Anexo 4 (Registros gráficos del centro de cómputos.) ____ *175*

Anexo 5 (Requisitos de RRHH para el acceso de proveedores) ____ *179*

Anexo 6 (Requisitos de MAHPI para el acceso de proveedores) ____ *180*

Anexo 7 (compromiso de confidencialidad) ____ *181*

Glosario y siglas. ____ *157*

Términos informáticos: ____ 182

Otros Términos: ____ 192

Bibliografía. ____ *193*

Introducción:

Frente a la perspectiva de seleccionar un tema y su enfoque para el desarrollo del trabajo final de graduación de la Licenciatura en Informática, me pareció importante que el mismo agregue valor a mi formación profesional haciendo un aporte concreto en la empresa donde trabajo.
Dada la responsabilidad que tengo como soporte técnico en la Planta Industrial que ARCOR tiene en Colonia Caroya, con más de ocho años de experiencia en el lugar, he encontrado diversos inconvenientes referidos a la seguridad informática. Por ejemplo, las personas comparten sus contraseñas; se utilizan y guardan en los servidores archivos de información de muy variados formatos; se instala software sin licencia; no hay restricción de accesos a los lugares donde se encuentran equipos críticos. Todo esto sin tener en cuenta los tiempos en que se utilizan los equipamientos informáticos para fines estrictamente personales ajenos a los productivos.
Recursos compartidos sin mediar una política, y otros disponibles: PCs, unidades de CD, disqueteras, hubs sin control y en algunos casos sin restricciones; descubren vulnerabilidades que podrían hacen posible amenazas, fallas o desperfectos.
También hay que considerar la posibilidad de intromisiones no autorizadas a la red, por ejemplo: algún intruso (proveedor o empleado) que pueda rastrear puertos para encontrar accesos a algún recurso de servidores o PCs críticas; o alguna otra vulnerabilidad de alguno de los sistemas operativos instalados en el sitio. Alguien interesado en buscar equipos, contraseñas o accesos restringidos, ya sea para curiosear o adueñarse de información.

A partir de estas apreciaciones he considerado hacer un relevamiento de situación desde el punto de vista de la seguridad informática en esta planta industrial de Arcor.
Luego, teniendo en cuenta diferentes consejos desde la teoría, haré un diagnóstico y una propuesta integradora.
Espero que este esfuerzo constituya un buen punto de partida para la reflexión y el debate sobre esta problemática en la organización.
Dada la amplitud del tema definiré claramente objetivos, alcances y límites para que el trabajo cumpla con los requisitos previstos por la Universidad Empresarial Siglo 21.

Antecedentes:

Se destaca que no hay algún antecedente en el cual se haya realizado análisis de seguridad informática en el sitio de Arcor en estudio. Tampoco se conoce que se hayan realizado ningún tipo de análisis de riesgos informáticos.

Sólo se pueden mencionar las siguientes acciones:

- Trabajos de seguridad sobre servidores realizados por Tecnología Informática de Arcor, septiembre de 2002.
- " Análisis sobre la aplicación de aspectos de seguridad a equipos informáticos SCADA (Sistemas de Control y Adquisición de Datos)." Materia: Práctica Profesional, Guillermo Young Barbé, julio de 2003.
- Aplicación efectiva de seguridad a equipos informáticos SCADA (Sistemas de Control y Adquisición de Datos) realizado por el soporte técnico local y un implementador de Tecnología Informática de Arcor, mayo 2003.

Descripción general sobre la problemática:

Para destacar la importancia y actualidad de la problemática de la seguridad informática, parece oportuno citar un artículo tomado del sitio www.bloggers.com.ar del 18/03/2004, donde en varios lugares se hace referencia al tema:

> "... Circular por Internet o simplemente estar conectado a clientes y proveedores se ha convertido en un riesgo que preocupa a las empresas. En la Argentina, en poco más de dos meses hay cuatro grandes encuentros internacionales sobre seguridad y guerra anti-spam."
>
> "El bombardeo de virus y otros ataques se ha convertido en una amenaza que desvela a millones de empresas y usuarios individuales en todo el mundo."
>
> "... cualquier red que esté conectada a Internet está sujeta a reiterados intentos de violación de su seguridad, lo cual obliga a fuertes inversiones en sistemas de protección." [1]

La preocupación se refleja en las diversas convocatorias internacionales. El tema de la seguridad es una de las estrellas en diversos eventos internacionales. Lo fue en Expocomm México y en la versión local realizada en Buenos Aires en septiembre de 2004. En la

[1] www.bloggers.com.ar (18/03/2004)

Provincia de Córdoba ya se realizó en abril de 2004 el "Congreso Iberoamericano de Auditoría, Seguridad y Forensia informática".
También se puede apreciar en las constantes advertencias contra virus que circulan por Internet y las propuestas de empresas como Microsoft de actualizar sus sistemas operativos con parches que protegen contra nuevas vulnerabilidades descubiertas.

> "Además de los ataques con virus y la invasión de correo basura, la preocupación de las empresas por la seguridad de sus redes ha trocado en obsesión..." [2]

En toda esta información se resalta claramente que la preocupación por la seguridad en las redes informáticas es más que importante y se convierte en un problema global y de actualidad.
Las organizaciones son cada vez más dependientes de sus redes informáticas y un problema que las afecte, por mínimo que sea, puede llegar a comprometer la continuidad de las operaciones.
La falta de medidas de seguridad en las redes es un problema que está en crecimiento. Cada vez es mayor el número de atacantes y cada vez están más organizados, por lo que van adquiriendo día a día habilidades más especializadas que les permiten obtener mayores beneficios.

Además no deben subestimarse las fallas de seguridad provenientes del interior mismo de la organización. Muchas de las amenazas y vulnerabilidades pueden surgir desde el mismo personal o de la multiplicidad de personas que ingresan y realizan trabajos internamente.
Como se menciona en la primera parte de esta introducción (página 6), ya se pueden entrever ciertas vulnerabilidades factibles de ser aprovechadas por personas mal intencionadas, por errores o por amenazas.
En la diversidad de áreas de la organización de la planta industrial hay interacción de las personas con los sistemas informáticos. En todas ellas hay riesgos sobre la seguridad informática que es conveniente medir, y reducir si fueran de consideración.

[2] www.bloggers.com.ar (18/03/2004)

Formulación del problema:

A partir de las observaciones de arriba, surge claramente un interrogante: ¿en qué situación de riesgo, desde el punto de vista de la seguridad de la información, se encuentra la planta industrial de Arcor en Colonia Caroya?

Justificación:

Considerando el interrogante anterior es de prioridad lograr establecer el estado de situación de la seguridad de la información.

La realización de un relevamiento, tomando patrones de estudio y guías para realizar análisis de riesgos, nos acercará a la realidad. Con esta visión surgirán, ciertamente, aspectos más críticos que otros que deberán ser estudiados con prioridad.

En el presente trabajo se prevé reducir el riesgo sobre la seguridad informática de dichos aspectos críticos.

También se pretende que el estudio que aquí se haga se pueda replicar en otras bases de Arcor, o al menos sirva para que se considere la realización de esquemas similares con cierta periodicidad.

Descripción de la Organización:

Arcor es el primer productor mundial de caramelos y el principal exportador de golosinas de Argentina, Brasil y Chile. Posee 31 plantas, 25 de las cuales están ubicadas en la Argentina y las 6 restantes en América Latina. Especializada en la elaboración de golosinas, chocolates, galletitas y alimentos, cuenta con un volumen de producción de más de 1 millón y medio de kilogramos diarios y llega con su propia marca a más de 100 países de los 5 continentes.

Exporta la más amplia variedad de productos siendo la empresa argentina que más mercados atiende a nivel global. En este contexto, Arcor fue rankeada por la Revista América Economía como uno de los grupos multinacionales más competitivos de Latinoamérica. En 2002, Luis Pagani, Presidente del Grupo Arcor, fue distinguido como "CEO del Año" por la revista norteamericana de negocios LatinFinance y en 2003 fue reconocido como "El Empresario de la Década" en el Premio Security y como "El mejor empresario agroindustrial" en el Premio a la Excelencia Agropecuaria (diario La Nación). A su vez, en el año 2003 Arcor alcanzó el puesto N° 1 en destacados rankings de prestigio empresario, como ser "Las 100 empresas con mejor imagen" (revista Apertura), "Las empresas con mayor transparencia empresaria" (revista Imagen), "Las 100 empresas más admiradas de la Argentina" (diario Clarín), y el ranking total de "Prestigio Empresario" (revista Prensa Económica), entre otros.

Fundada el 5 de julio de 1951, Arcor es líder en golosinas, chocolates y alimentos en Argentina, logro alcanzado a través de una reinversión constante de utilidades, que en la última década ha superado los U$S 1000 millones.
Gracias a este esfuerzo, hoy puede mostrar con orgullo plantas que se ubican a la vanguardia mundial en tecnología, como la de chocolates de Colonia Caroya, en Córdoba; la de galletitas en Salto, Buenos Aires, primera planta alimenticia argentina en recibir la certificación IRAM 3800, y catalogada por los expertos como modelo en su género; o como las de Perú y Chile. En marzo de 1999, se inauguró la planta de chocolates en Bragança Paulista, Brasil. Y en diciembre de 2000 se construyó un centro de distribución en Chile, uno de los más importantes del país.
Apostando a una nueva inserción de la industria argentina y de la región en el mundo, el Grupo mantiene un compromiso constante con la calidad e innovación, reflejado en el lanzamiento de más de 100 nuevos productos por año.

La obsesión por la calidad ha llevado a Arcor a ser una de las primeras empresas de su sector - y de la industria en general- en certificar sus procesos productivos con las normas internacionales de calidad ISO 9.000 y ambientales ISO 14.001, ocupando el primer puesto en el ranking Clarín, realizado por CEOP, en la categoría "Calidad y Medio Ambiente" durante 3 años en forma consecutiva (años 2000, 2001 y 2002).

Objetivo:

Determinar la situación actual referente a la Seguridad Informática, en el ámbito de la planta industrial de ARCOR - División Chocolates de Colonia Caroya.

Realizar una propuesta de solución sobre los aspectos que resulten del análisis anterior como prioritarios.

Alcances del trabajo:

?? Se relevará la situación actual en que se encuentra la planta de Arcor en Colonia Caroya desde el punto de vista de la seguridad informática.

?? Se realizará una investigación de los aspectos teóricos a tener en cuenta sobre seguridad informática.

?? Se diagnosticará la situación cruzando y comparando la información obtenida en los puntos anteriores.

?? Se realizará una propuesta integradora sobre los aspectos que resulten del análisis anterior como prioritarios.

?? Se establecerán pautas o procedimientos de seguridad que deben cumplir los nuevos proyectos informáticos que se pretendan implementar en el sitio.

Limites:

Desde el relevamiento y diagnóstico de la Seguridad Informática de la planta Industrial en Colonia Caroya hasta la propuesta de solución. Cabe aclarar que dicha propuesta se limitará a los aspectos que surjan como prioritario desde el diagnóstico.

Marco Teórico.

Los interrogantes que surgen cuando se pretende aplicar un diagrama de seguridad informática son: qué se está protegiendo, de quién y de qué hay que protegerlo.[3]
Es importante resaltar que el gran protagonista de la Seguridad Informática es la información. Y su objetivo será mantener la Integridad, Disponibilidad, Privacidad (aspectos fundamentales), Control y Autenticidad de la información manejada por computadoras.
Siguiendo esta línea he recopilado los aspectos de la información y sus atributos esenciales. Se detalla qué cuidados y precauciones hay que tener y se resalta la importancia de la realización de análisis de riesgos completos y periódicos.
He enumerado qué proteger, de quién y contra qué protegerse y cuáles son los costos y hasta que punto conviene invertir para lograr una seguridad aceptable.
También se muestra detalladamente qué aspectos debe incluir un análisis de riesgo y se enumeran los aspectos de seguridad informática a monitorear.

¿Qué es la información y cuáles son sus atributos?

Para comenzar el análisis de la Seguridad Informática se deberá tener en cuenta las características de lo que se pretende proteger: la Información.

"La información es una agregación de datos que tiene un significado específico más allá de cada uno de estos"[4]

Establecer el valor de la información es algo totalmente relativo, pues constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, las aplicaciones y la documentación.

Existe Información que debe o puede ser **pública**: puede ser visualizada por cualquier persona (por ejemplo índice de analfabetismo en un país); y aquella que **debe ser privada**: sólo puede ser visualizada por un grupo selecto de personas que trabaja con ella (por ejemplo antecedentes médicos). En esta última debemos maximizar nuestros esfuerzos para preservarla de ese modo reconociendo las siguientes características en la Información:

1. Es Crítica: es indispensable para garantizar la continuidad operativa.

[3] POBLACIÓN, Martín; apuntes de "Seguridad Informática", Universidad Empresarial Siglo 21, marzo de 2003.
[4] CALVO, Rafael Fernández. Glosario Básico Inglés-Español para usuarios de Internet. 1994-2000. http://www.ati.es/novatica/2000/145 - abril de 2004

2. Es Valiosa: es un activo con valor en sí misma.
3. Es Sensitiva: debe ser conocida por las personas que la procesan y sólo por ellas.

Uno de los atributos de la información: la SEGURIDAD.

La seguridad de la información se define como la preservación de las siguientes características principales:

La **Integridad** de la Información es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorias. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema.

La **Disponibilidad** u **Operatividad** de la Información es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria.

La **Privacidad o Confidencialidad** de la Información es la necesidad de que la misma sólo sea conocida por personas autorizadas. En casos de falta de confidencialidad, la Información puede provocar severos daños a su dueño (por ejemplo conocer antecedentes médicos de una persona) o volverse obsoleta (por ejemplo: los planes de desarrollo de un producto que se "filtran" a una empresa competidora, facilitarán a esta última desarrollar un producto de características semejantes).

Adicionalmente se valoran también la protección de los siguientes atributos de la información:

La **Consistencia** asegura que el sistema se comparta como lo esperan los usuarios autorizados.

El **Control** sobre la información permite asegurar que sólo los usuarios autorizados pueden decidir cuando y como permitir el acceso a la misma.

La **Autenticidad** permite definir que la información requerida es válida y utilizable en tiempo, forma y distribución. Esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades.

La **Protección a la Réplica** permite asegurar que una transacción sólo puede realizarse una vez, a menos que se especifique lo contrario. No se deberá poder grabar una transacción para

luego reproducirla, con el propósito de copiar la transacción para que parezca que se recibieron múltiples peticiones del mismo remitente original.
El **No Repudio** evita que cualquier entidad que envió o recibió información alegue, ante terceros, que no la envió o recibió.
La **Auditoría** determina qué, cuándo y quién realiza acciones o procesos sobre el sistema.

¿Qué se requiere para proveer de una seguridad efectiva?

Es de importancia realizar un acercamiento comprensivo e integral que considere una variedad de áreas dentro y fuera del ámbito de la seguridad informática.
Los controles de seguridad frecuentemente dependen del funcionamiento adecuado de otros controles (administrativos, técnicos, operativos). Existen muchas interdependencias y por lo tanto sin un firme conocimiento de ellas, algunos controles pueden interferir sobre otros. La seguridad informática necesita trabajar en conjunto con otras disciplinas de seguridad tradicionales, incluyendo la física y la personal.

A través de la selección y aplicación de medidas de **seguridad adecuada**, la seguridad ayuda a la realización de la misión de la organización, protegiendo sus recursos físicos y financieros, reputación, posición legal, empleados y otros aspectos tanto tangibles como intangibles.
"La seguridad es un medio para un fin y no un fin en sí mismo."
Es necesario comprender la misión de la organización y cómo cada sistema de información participa en el soporte de la misma. Esto asigna a cada sistema un rol y podemos definir los requerimientos de seguridad implícitos a éste.

La seguridad informática es un elemento integral de la buena administración. Incluir consideraciones de seguridad en la gestión de la información y los sistemas tecnológicos asegura la protección de otros recursos de la organización (financieros, empleados, reputación, etc.). sin embargo, no elimina completamente la posibilidad de que estos elementos valiosos sean dañados.
En última instancia, los gerentes de la organización tendrán que decidir que nivel de riesgo están dispuestos a aceptar, teniendo en cuenta los costos de los controles de seguridad.

Cabe definir **Amenaza**, en el entorno informático, como cualquier elemento que comprometa al sistema.

Las amenazas pueden ser analizadas en tres momentos: antes, durante o después del ataque. Estos mecanismos conformarán políticas que garantizarán la seguridad de nuestro sistema informático.

a. **La Prevención (antes):** mecanismos que aumentan la seguridad (o fiabilidad) de un sistema durante su funcionamiento normal. Por ejemplo el cifrado de información para su posterior transmisión.

b. **La Detección (durante):** mecanismos orientados a revelar violaciones a la seguridad. Generalmente son programas de auditoría.

c. **La Recuperación (después):** mecanismos que se aplican, cuando la violación del sistema ya se ha detectado, para retornar éste a su funcionamiento normal. Por ejemplo recuperación desde las copias de seguridad (backup) realizadas.

Las preguntas que se hace un técnico en sistemas de información ante un problema de seguridad, normalmente, están relacionadas con medidas defensivas que no solucionan un problema dado, sólo lo transforma o retrasa. La amenaza o riesgo sigue allí y las preguntas que este técnico debería hacerse son:

- ¿Cuánto tardará la amenaza en superar la "solución" planteada?
- ¿Cómo se hace para detectarla e identificarla a tiempo?
- ¿Cómo se hace para neutralizarla?

Para responderlas definimos **Riesgo** como "la proximidad o posibilidad de daño sobre un bien".

Ya se trate de actos naturales, errores u omisiones humanas y actos intencionales, cada riesgo debería ser atacado de las siguientes maneras:

1. Minimizando la posibilidad de su ocurrencia.
2. Reduciendo al mínimo el perjuicio producido, si no ha podido evitarse que ocurriera.
3. Diseño de métodos para la más rápida recuperación de los daños experimentados.
4. Corrección de las medidas de seguridad en función de la experiencia recogida.

Luego, el **Daño** es el resultado de la amenaza; aunque esto es sólo la mitad del axioma.

El daño también es el resultado de la no–acción, o acción defectuosa, del responsable de la seguridad informática (que desde ahora lo llamaré protector). El daño puede producirse porque el protector no supo identificar adecuadamente la amenaza y, si lo hizo, se impusieron

criterios comerciales por encima de los de seguridad. De allí que se deriven responsabilidades para la amenaza pero también para la figura del protector.
Luego, el protector será el encargado de detectar cada una de las **Vulnerabilidades** (debilidades) del sistema que pueden ser explotadas y empleadas, por la amenaza, para comprometerlo. También será el encargado de aplicar las **Contramedidas** (técnicas de protección) adecuadas. La Seguridad indicará el índice en que un Sistema Informático está libre de todo peligro, daño o riesgo. Esta característica es muy difícil de conseguir o imposible en un 100% por lo que sólo se habla de **Fiabilidad** y se la define como "la probabilidad de que un sistema se comporte tal y como se espera de él", y se habla de Sistema Fiable en vez de sistema seguro.
Luego para garantizar que un sistema sea fiable se deberá garantizar las características ya mencionadas de Integridad, Operatividad, Privacidad, Control y Autenticidad. Se deberá conocer "qué es lo que queremos proteger", "de quién lo queremos proteger", "cómo se puede lograr esto legislativa y técnicamente"; para luego concluir con la formulación de estrategias adecuadas de seguridad tendientes a la disminución de los riesgos.
Comprender y conocer de seguridad ayudará a llevar a cabo análisis sobre los Riesgos, las Vulnerabilidades, Amenazas y Contramedidas; evaluar las ventajas o desventajas de la situación; a decidir medidas técnicas y tácticas metodológicas, físicas, e informáticas, en base de las necesidades de seguridad.

De aquí surgen temas importantes a considerar en éste marco referencial: el **análisis de riesgo**, la **relación operatividad – seguridad** y el análisis de **costo – beneficio** para asegurar que los costos de protección no excedan los beneficios esperados.

Aspectos de Seguridad Informática:

Basado en los puntos teóricos anteriores y buscando información en diferentes fuentes[3,4] he realizado la siguiente lista sobre la cual se debería analizar una organización para confeccionar un programa de Seguridad Informática acorde a la misma:

- Primera clasificación:
  - Seguridad Física;
  - Seguridad Lógica

- Segunda clasificación, desde el punto de vista de amenazas, vulnerabilidades, ataques:
  - Errores y omisiones;
  - Fraude y robo;
  - Sabotaje de los empleados;
  - Pérdida de soporte físico y de infraestructura;
  - Actividades de hackers malintencionados (Crackers);
  - Ejecución de código malicioso;
  - Espionaje industrial;
  - Amenazas a la privacidad personal;
  - Aspectos de Ingeniería social.

- Tercera clasificación: Intrusos:
  - Hacker, Cracker;
  - Personal interno de la empresa;
  - Ex empleados,
  - Curiosos,
  - Terroristas;
  - Intrusos remunerados.

- Virus informáticos.

- Usos inadecuados de los recursos informáticos de la compañía:
  - Navegación indiscriminada y sin control en Internet;
  - Uso de archivos de todo tipo, ajenos a la actividad productiva;

Detalles de los puntos indicados en la lista precedente:

Seguridad física:

Las principales amenazas que se prevén en Seguridad Física son:

1. Desastres naturales, incendios accidentales, tormentas e inundaciones
2. Amenazas ocasionadas por el hombre
3. disturbios, sabotajes internos y externos deliberados.

Seguridad Lógica:

Los objetivos que se plantean serán:

[3,4] Op. cit. pág. 13; Op. cit. pág. 14

- ?? Restringir el acceso a los programas y archivos
- ?? Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- ?? Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.
- ?? Que la información transmitida sea recibida por el destinatario al cual ha sido enviada y no a otro.
- ?? Que la información recibida sea la misma que ha sido transmitida.
- ?? Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- ?? Que se disponga de pasos alternativos de emergencia para la transmisión de información.

Errores y Omisiones:

Afectan a la integridad de los datos o del sistema. Pueden ser causados por usuarios, operadores o programadores. En algunos casos el error es la amenaza, otras veces crea nuevas vulnerabilidades.

Fraude y robo:

Puede ser causado por usuarios externos o internos, aunque son éstos últimos los que más riesgo representan por su conocimiento de la estructura de la organización.

Sabotaje de los empleados:

Se pueden dar en número menor al robo y fraude, pero son de un costo muy elevado. La motivación del sabotaje puede ir desde el altruismo a la venganza pasando también por el beneficio propio.

Pérdida de soporte físico y de infraestructura:

Este aspecto está relacionado con la seguridad física. Por ejemplo ante cortes de energía eléctrica por tiempo prolongado o la falla del sistema de aire acondicionado. También puede darse el caso que ante una inundación o amenaza similar los empleados no puedan concurrir al centro de cómputos aunque esté protegido y permanezca operacional.

Actividades de hackers malintencionados (Crackers):

Pueden ser internos o externos En el caso de los externos, no se rigen por las reglas de la organización. La mayoría de las veces permanecen anónimos. Como no se pueden conocer sus verdaderas motivaciones se puede sugerir que no tienen limitaciones.

Ejecución de código malicioso:

Las computadoras están diseñadas para ejecutar instrucciones una después de la otra. Estas instrucciones, generalmente hacen algo útil. Sin embargo a veces las instrucciones ejecutadas pueden ser dañinas o maliciosas en su naturaleza. A veces se utiliza el término malware para describir amenazas maliciosas.

Espionaje industrial:

La seguridad informática puede ayudarnos a proteger los sistemas y datos contra esta amenaza, pero poco puede hacer para evitar que un usuario autorizado venda esta información.

Amenazas a la privacidad personal:

La acumulación de grandes cantidades de información acerca de los individuos por parte del gobierno, organismos crediticios y organizaciones privadas y la capacidad de los sistemas de controlar y procesar constituyen una amenaza a la privacidad de las personas.

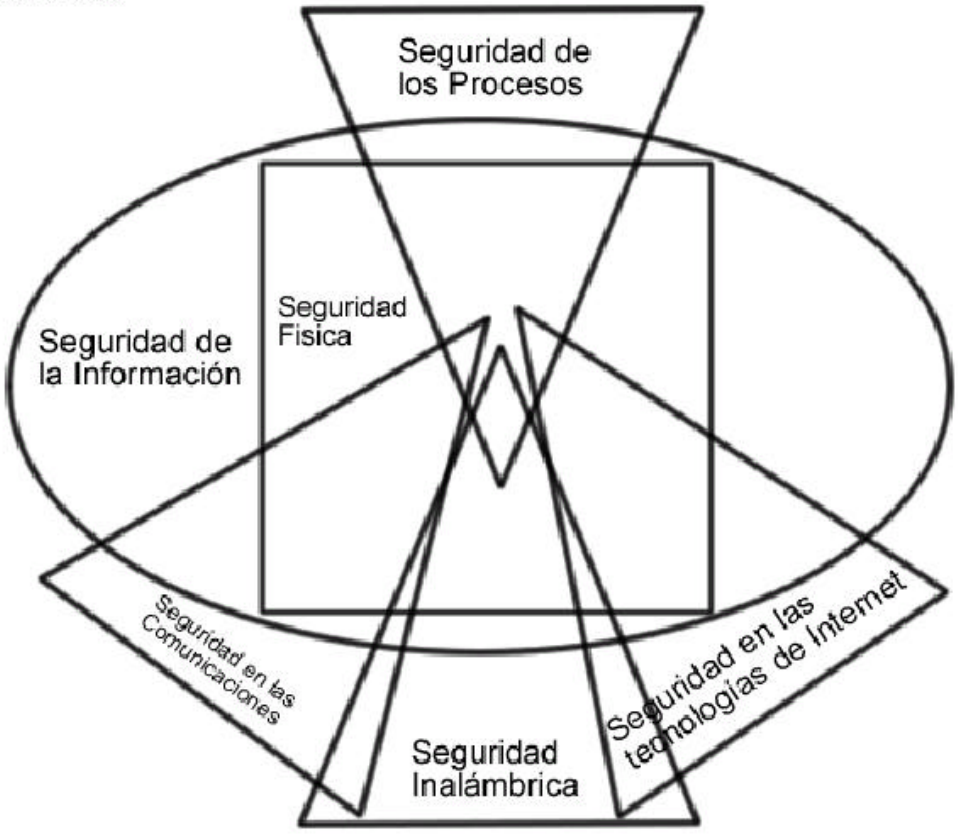
Aspectos de ingeniería social:

Se denomina ingeniería social a todo artilugio, tretas o técnicas elaboradas a través del engaño de las personas, para revelar contraseñas u otra información. Es previa a la obtención de dicha información a través de las debilidades propias de una implementación y mantenimiento de un sistema.

Mapa de Seguridad[5]

El mapa de seguridad es un esquema de la presencia de seguridad. Corresponde al ambiente de un análisis de seguridad y se compone por seis secciones. Las secciones se superponen entre sí y contienen elementos de todas las otras secciones. Un análisis apropiado de cualquier sección debe incluir los elementos de todas las otras secciones, directa o indirectamente.

1 Seguridad de la Información
2 Seguridad de los Procesos
3 Seguridad en las tecnologías de Internet
4 Seguridad en las Comunicaciones
5 Seguridad Inalámbrica
6 Seguridad Física



Lista de Módulos del Mapa de Seguridad

La lista de módulos del mapa de seguridad son los elementos primarios de cada sección. Cada módulo debe incluir todas las Dimensiones de Seguridad que están integradas con tareas a ser desarrolladas. Para desarrollar un análisis de seguridad OSSTMM[6] de una sección particular, todos los módulos de la sección deben ser desarrollados y aquellos para los que no exista infraestructura y no pueda ser verificada, debe definirse como NO APLICABLE.

1. **Seguridad de la Información**

[5] Manual de Seguridad de ArCERT: Coordinación de Emergencia en Redes Teleinformáticas.
[6] HERZOG Pete; Manual de la Metodología Abierta de Testeo de Seguridad OSSTMM 2.1- 23 de agosto de 2003; ISECOM (Institute For SECurity And Open Methodologies)

i. Revisión de la Inteligencia Competitiva
ii. Revisión de Privacidad
iii. Recolección de Documentos
iv. Seguridad de los Procesos
v. Testeo de Solicitud
vi. Testeo de Sugerencia Dirigida
vii. Testeo de las Personas Confiables

2. **Seguridad en las tecnologías de Internet**
   i. Logística y Controles
   ii. Sondeo de Red
   iii. Identificación de los Servicios de Sistemas
   iv. Búsqueda de Información Competitiva
   v. Revisión de Privacidad
   vi. Obtención de Documentos
   vii. Búsqueda y Verificación de Vulnerabilidades
   viii. Testeo de Aplicaciones de Internet
   ix. Enrutamiento
   x. Testeo de Sistemas Confiados
   xi. Testeo de Control de Acceso
   xii. Testeo de Sistema de Detección de Intrusos
   xiii. Testeo de Medidas de Contingencia
   xiv. Descifrado de Contraseña
   xv. Testeo de Denegación de Servicios
   xvi. Evaluación de Políticas de Seguridad
3. **Seguridad en las Comunicaciones**
   i. Testeo de PBX
   ii. Testeo del Correo de Voz
   iii. Revisión del FAX
   iv. Testeo del Módem
4. **Seguridad Inalámbrica**
   i. Verificación de Radiación Electromagnética (EMR)
   ii. Verificación de Redes Inalámbricas [802.11]
   iii. Verificación de Redes Bluetooth
   iv. Verificación de Dispositivos de Entrada Inalámbricos
   v. Verificación de Dispositivos de Mano Inalámbricos
   vi. Verificación de Comunicaciones sin Cable
   vii. Verificación de Dispositivos de Vigilancia Inalámbricos
   viii. Verificación de Dispositivos de Transacción Inalámbricos
   ix. Verificación de RFID
   x. Verificación de Sistemas Infrarrojos
   xi. Revisión de Privacidad
5. **Seguridad Física**
   i. Revisión de Perímetro
   ii. Revisión de monitoreo
   iii. Evaluación de Controles de Acceso
   iv. Revisión de Respuesta de Alarmas
   v. Revisión de Ubicación
   vi. Revisión de Entorno

El propósito es elaborar una lista de vulnerabilidades (debilidades o fallas) que puedan ser explotadas por fuentes de amenaza potenciales.

Un método recomendado para identificar las vulnerabilidades es utilizar listas de vulnerabilidades conocidas, analizar la performance del sistema de seguridad propio y el desarrollo de una lista de requerimientos de seguridad.

Análisis de riesgo:

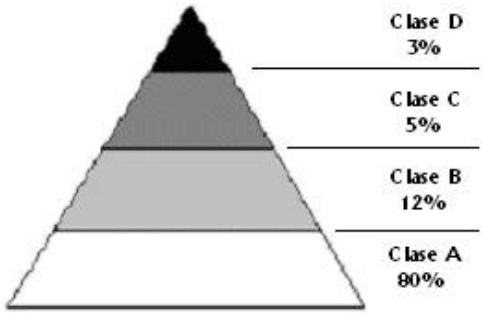
"Es la evaluación de las amenazas, impactos y vulnerabilidades relativos a la información y a las instalaciones de procesamientos de la misma, y a la probabilidad de que ocurran" (Norma IRAM 17799)

El análisis de riesgo es una parte muy importante del proceso de Seguridad Informática. Para proteger algo se debe saber qué y contra qué protegerlo. Todos los datos que sean recopilados sirven de soporte para una evaluación válida.
Una vez evaluados los riesgos se podrán plantear políticas y técnicas de protección.

Por lo tanto:

¿De quién debemos protegernos?

Se llama Intruso o Atacante a la persona que accede (o lo intenta) sin autorización a un sistema ajeno, ya sea en forma intencional o no.
Podemos ver los tipos de intrusos existentes desde el punto de vista del nivel de conocimiento en el siguiente esquema:



Tipos de Intrusos. Fuente: CybSec S.A. http://www.cybsec.com (marzo de 2004)

1. Clase A: el 80% en la base son los nuevos intrusos que bajan programas de Internet y prueban, están jugando (...) son pequeños grupitos que se juntan y dicen vamos a probar.
2. Clase B: es el 12% son más peligrosos, saben compilar programas aunque no saben programar. Prueban programas, conocen como detectar que sistema operativo está usando la víctima, testean las vulnerabilidades del mismo e ingresan por ellas.
3. Clase C: es el 5%. Es gente que sabe, que conoce y define sus objetivos. A partir de aquí buscan todos los accesos remotos e intentan ingresar.

4. Clase D: el 3% restante. Cuando entran a determinados sistemas buscan la información que necesitan.

   Para llegar desde la base hasta el último nivel se tarda desde 4 a 6 años, por el nivel de conocimiento que se requiere asimilar. Es práctica, conocer, programar, mucha tarea y mucho trabajo.

¿Qué se debe proteger?

Hay tres elementos básicos a proteger:

- ?? Hardware: todos los elementos físicos del sistema: servidores, estaciones de trabajo, impresoras, activos de red, cableado eléctrico y de red, etc.
- ?? Software: Elementos lógicos que hacen funcional al hardware: sistemas operativos, aplicaciones, herramientas de desarrollo, etc.
- ?? Datos: Información que maneja el sistema: bases de datos, documentos de correo electrónico, documentación de sistemas, manuales de usuario, procedimientos operativos, documentos de usuarios, etc.

Los datos que maneja el sistema serán el elemento más importante ya que son el resultado del trabajo realizado. Si existiera daño del hardware o software, estos pueden adquirirse nuevamente desde su medio original; pero los datos obtenidos en el transcurso del tiempo por el sistema son imposibles de recuperar. Obligatoriamente se debe disponer de un sistema de copias de seguridad, y aún así será difícil de devolver los datos a su forma anterior al daño.

¿Contra qué debe protegerse?

Para cualquiera de los elementos descriptos existen multitud de amenazas y ataques que se los puede clasificar en:

1. Ataques Pasivos: el atacante no altera la comunicación, sino que únicamente la "escucha" o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico. Generalmente se emplean para:

- Obtención del origen y destinatario de la comunicación, a través de la lectura de las cabeceras de los paquetes monitorizados.
- Control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales.

- Control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad. Mediante el cifrado de la información y otros medios es posible evitar el éxito, aunque no el ataque.

2. Ataques Activos: estos ataques implican algún tipo de modificación del flujo de datos transmitido o creando un falso flujo de datos. Generalmente son realizados por hackers, piratas informáticos o intrusos remunerados y se los puede subdividir en cuatro categorías:

- Interrupción: si hace que un objeto del sistema se pierda, quede inutilizable o no disponible.
- Intercepción: si un elemento no autorizado consigue el acceso a un determinado objeto del sistema.
- Modificación: si además de conseguir el acceso consigue modificar el objeto.
- Fabricación: se consigue un objeto similar al original atacado de forma que es difícil distinguirlos entre sí.
- Destrucción: es una modificación que inutiliza el objeto.

Entre los métodos de ataques más comunes se encuentran:

Ataques de Diccionario o Fuerza Bruta. La técnica más utilizada es el cracking de contraseñas y el exploit de vulnerabilidades conocidas. Permite conseguir acceso al sistema utilizando la cuenta de otra persona aprovechando que los usuarios por lo general utilizan contraseñas débiles.

Denegación de Servicios (DoS). Es el resultado de inundar la red con mensajes no solicitados o cuando un gusano se propaga y toma control de la totalidad de la misma.

Network Spoofing. Cuando un sistema se presenta en la red como si fuera otro sistema.

Secuencia de un ataque.

Un ataque típico a un equipo conectado o no a una red puede desglosarse en los siguientes pasos:

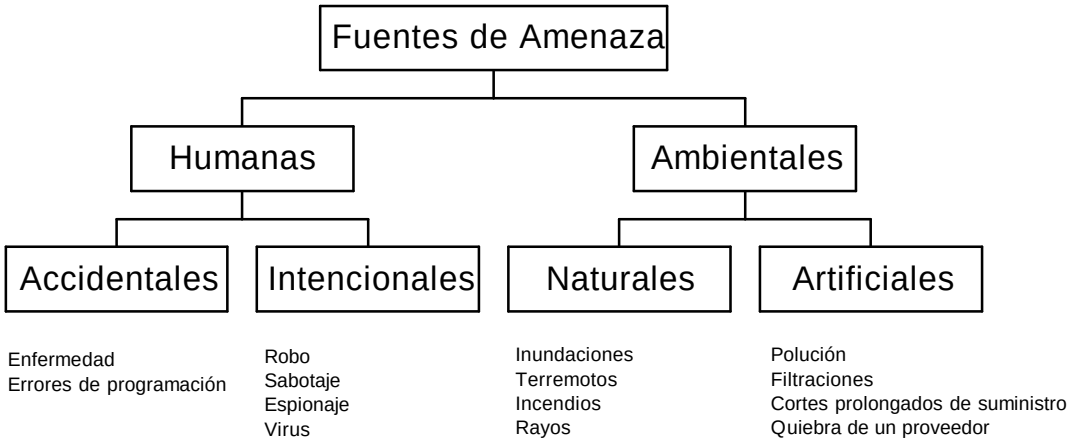
1. **Localizar el objetivo.** Por ejemplo, puede ser una búsqueda a nivel de red utilizando herramientas de barrido o consultas de bases de datos de registro de dominios.
2. **Obtención de información.** Se puede hacer una identificación del sistema operativo, servicios o procesos que se están ejecutando y si presentan vulnerabilidades conocidas.
3. **Acceso remoto/local.** Puede ser mediante la obtención de una cuenta en el equipo, la ejecución de un troyano, exploit, etc.

4. **Escalada de privilegios.** Consiste en la obtención de privilegios de administrador mediante cracking de contraseñas, programas setuserid, etc.
5. **Borrado de huellas.** Se procede a la modificación de los archivos de registro a fin de eliminar todo rastro de la intrusión.
6. **Mantener el acceso.** Se instalan programas o crean cuentas para facilitar o mantener el acceso en próximas ocasiones.

Con demasiada frecuencia se cree que los piratas son lo únicos que amenazan nuestro sistema, siendo pocos los administradores que consideran todos los demás riesgos analizados en el presente.

Para cada elemento a asegurar: hardware, software o datos, existen múltiples tipos de amenazas. Algunas amenazas son comunes y otras propias de cada uno de ellos.

Clasificación general de las fuentes de amenazas:



También se puede clasificar las amenazas como internas o internas.

Pero lo más importante es hacer una lista de amenazas de acuerdo a la organización y su entorno.

Otra clasificación de Riesgos[7]

Vulnerabilidad:

Una falla inherente en el mecanismo de seguridad mismo o que pueda ser alcanzada por medio de protecciones de seguridad. Falla que permite el acceso privilegiado a la ubicación,

[7] HERZOG, Pete; Manual de la Metodología Abierta de Testeo de Seguridad OSSTMM 2.1- 23 de agosto de 2003; ISECOM (Institute For SECurity And Open Methodologies)

gente, procesos del negocio, y personal o acceso remoto a los procesos, gente, infraestructura generando datos corruptos o eliminados. Una vulnerabilidad puede ser un metal en una puerta que se torna frágil a temperaturas bajo 0º C; un lector de huellas digitales que permite el acceso con dedos de goma; un dispositivo infrarrojo que no tiene mecanismos de autenticación para realizar cambios en la configuración; o un error de traducción en un servidor web que permite la identificación del propietario de una cuenta bancaria por medio del número de esta.

Debilidad:

Una falla inherente a la plataforma o ambiente en el que el mecanismo de seguridad reside, una mala configuración, falla de sobre vivencia, falla de usabilidad, o falla al cumplir los requerimientos de una Política de Seguridad. Una debilidad puede ser un proceso que no almacena datos transaccionales durante el tiempo límite legal, tal y como se establezca en las leyes locales; una alarma de ingreso que no suena si la puerta ha quedado abierta por un período de tiempo específico; un firewall que devuelve mensajes ICMP de host inalcanzable para sistemas de red internos; un servidor de base de datos que permite consultas sin filtrar; una entrada sin monitoreo a un edificio considerado "seguro".

Filtrado de Información:

Una falla inherente en el mecanismo de seguridad mismo, o que puede ser alcanzada por medio de medidas de seguridad que permiten el acceso privilegiado a información sensitiva o privilegiada acerca de datos, procesos de negocio, personal o infraestructura. Una fuga de información puede ser una cerradura con la combinación disponible por medio de señales audibles de cambio dentro de los mecanismos de la misma; un enrutador que brinda información SNMP acerca de la red objetivo; una hoja de cálculo con los salarios de ejecutivos en una compañía privada; el teléfono celular privado del personal de seguridad; un sitio web con información acerca de la próxima revisión del elevador de la compañía.

Preocupación:

Un evento de seguridad que puede resultar al no seguir las practicas recomendadas de seguridad, y que por el momento no se presente como un peligro actual. Una preocupación puede ser el de determinado servicio corriendo en un servidor de la organización cuando no requiere el servicio; una puerta de entrada vigilada que requiere que el celador deje la puerta

para perseguir a un intruso y no se disponga de un nuevo celador haciendo presencia en la misma puerta; o empleados que se sientan con sus monitores y tableros visibles desde el exterior del perímetro de seguridad.

Desconocidos:

Un elemento desconocido o sin identificación en el mecanismo de seguridad mismo, o que puede ser alcanzado a través de las medidas de seguridad y actualmente no tiene impacto conocido en la seguridad ya que tiende a no tener sentido o sirva a ningún propósito con la información limitada que el analista posea. Un desconocido puede ser una respuesta inesperada posiblemente de un enrutador en una red, indicando problemas en la misma; una frecuencia de radio no natural que proviene del perímetro de seguridad sin ofrecer información o identificación; o una hoja de cálculo con información privada acerca de la competencia.

Relación Operatividad–Seguridad

Seleccionar las medidas de seguridad a implantar requiere considerar el equilibrio entre los intereses referidos a la seguridad, los requerimientos operacionales y la "amigabilidad" para el usuario.

Imaginemos una computadora “extremadamente” segura:

Instalada a 20 metros bajo tierra en un recinto de hormigón.

Aislada informáticamente de otras computadoras.

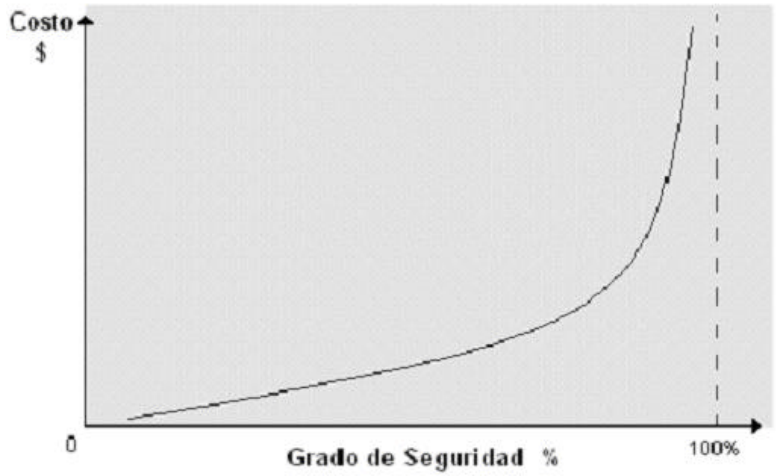
Aislada eléctricamente y alimentada por un sistema autónomo de triple reemplazo.

Ahora imaginemos la utilidad de está “super segura” computadora: tendiente a nula.

Con esto refleja que la Seguridad y la Utilidad de una computadora son inversamente proporcionales; es decir que al incrementar la seguridad en un sistema informático, su operatividad desciende y viceversa.

$$\text{Seguridad} \propto \frac{1}{\text{Operatividad}}$$

Para mantener el grado de seguridad del ejemplo, los costos crecen exponencialmente al acercarse al 100% de seguridad.



[8]

Más allá de ello, al tratarse de una ciencia social, no determinística, se mantendrá la incertidumbre propia del comportamiento humano, que puede permitir a un atacante violar el sistema, haciendo que los costos hayan sido, si bien no inútiles, excesivos.

Debemos recordar que el concepto de Seguridad es relativo, pues no existe una prueba total contra engaños, sin embargo existen niveles de seguridad mínimos exigibles.
Este nivel dependerá de un análisis de los riesgos que estamos dispuestos a aceptar, sus costos y de las medidas a tomar en cada caso.

Para ubicarnos en la vida real, veamos los datos obtenidos en marzo de 2001 por la consultora Ernst & Young sobre 273 empresas de distintos sectores de actividad y países.

- El 40% de las empresas estudiadas consideran como un problema grave la seguridad informática.
- El "gasto" en Seguridad Informática oscila entre el 4% y el 10% del gasto total informático.
- El 83% de las empresas reconoce no haber emprendido nunca acciones legales después de un ataque.
- El 72% se muestra reacia a admitir que sus sistemas han sido saboteados.
- El 79% cree que existen mayores probabilidades de sufrir un ataque informático procedente del exterior. (Luego veremos que esto es un error.)

[8] ALDEGANI, Gustavo. Miguel. Seguridad Informática. MP Ediciones. 1° Edición. Argentina. 1997. Página 26.

- El 66% consideran a la Seguridad y Privacidad de la información el impedimento principal para el crecimiento del comercio electrónico.
- El 80% manifestó no haber experimentado un ataque por intrusión durante el año anterior; pero sólo el 33% indicó su capacidad para la detección de dichos ataques.
- Sólo el 39% hace uso de software estándar de seguridad y el 20% de este total hace uso avanzado de estas herramientas.

¿Cuánto tiempo, dinero y esfuerzo se está dispuesto a invertir para obtener una protección adecuada?

Se debe asignar a cada riesgo un costo y determinar el costo para defenderse.

Se trata de **costos de las pérdidas** y el **costo de prevención** que debe amortizarse a lo largo de la vida esperada de aquello protegido.

Para cada riesgo, además del costo, se le asocia una probabilidad estimada de ocurrencia y un costo de recuperación del daño.

El objetivo debe ser evitar pérdidas caras y probables antes de preocuparse de pérdidas menos probables y de poco costo.

La seguridad debe ser apropiada y a la vez proporcional al valor y grado de dependencia de los sistemas de Tecnología Informática, pero también a la severidad, probabilidad y extensión de un potencial daño.

Del Manual de Seguridad de ArCERT: Coordinación de Emergencia en Redes Teleinformáticas he extraído la siguiente recomendación que tiene mucho en común con el planteo anterior:

> "Se comienza realizando una evaluación del **factor humano** interviniente - teniendo en cuenta que éste es el punto más vulnerable en toda la cadena de seguridad -, de los **mecanismos** con que se cuentan para llevar a cabo los procesos necesarios (mecanismos técnicos, físicos ó lógicos), luego, el **medio ambiente** en que se desempeña el sistema, las consecuencias que puede traer aparejado defectos en la seguridad (pérdidas físicas, pérdidas económicas, en la imagen de la organización, etc.), y cuáles son las **amenazas posibles**.
>
> Una vez evaluado todo lo anterior, se origina un programa de seguridad, que involucra los pasos a tomar para poder asegurar el umbral de seguridad que se desea. Luego, se pasa al plan de acción, que es cómo se va a llevar a cabo el programa de seguridad. Finalmente, se redactan los procedimientos y normas que permiten llegar a buen destino."[9]

[9] Manual de Seguridad de ArCERT: Coordinación de Emergencia en Redes Teleinformáticas.

Métodos y guías de análisis sobre seguridad informática.

Guías MAGERIT[10]

Objetivos de MAGERIT

- Estudiar los riesgos que soporta un sistema de información y el entorno asociado a él. MAGERIT propone la realización de un análisis de los riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en la organización; señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados.
- Los resultados del análisis de riesgos permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.
- Como objetivo a más largo plazo, MAGERIT prepara su lógica articulación con los mecanismos de evaluación, homologación y certificación de seguridad de sistemas de información (ITSEC, Criterios Comunes de Evaluación de la Seguridad de los Productos y Sistemas de Información).

Pasos sugeridos por MAGERIT (Abr 11/72 Medidas preventivas mínimas de seguridad).

- Identificar activos importantes relacionados con la información.

  Evaluación organizacional. Basado en el conocimiento de la misión de la empresa, las distintas áreas, y en lo que se considera importante por los responsables. Se arma una lista y se asigna un valor de prioridad a fin de identificar los activos más importantes (activo crítico).

  Requerimientos de seguridad asociados. Se enfoca el análisis en estos activos y se identifican cuales son los requerimientos de seguridad (confidencialidad, integridad, disponibilidad...) para cada uno.

[10] MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) http://www.csi.map.es/csi/pg5m20.htm - septiembre de 2004

- Identificar una lista de amenazas para cada activo.

- Buscar vulnerabilidades en la infraestructura.

  Evaluación tecnológica de la infraestructura que sirve de soporte a los activos críticos.

- Desarrollar estrategias y planes de seguridad.

  Evaluación de riesgos.
  Selección de controles. Políticas.
- Implementar, controlar, auditar, actualizar.

Los Activos son "recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección". (Guía de Aproximación a la Seguridad de los Sistemas de Información, de MAGERIT, Pág. 16).

Las Guías MAGERIT clasifican los activos en 5 categorías.

1. El **entorno** del Sistema de Información necesario para su funcionamiento: instalación física, infraestructura de comunicaciones y otras, suministros, personal operacional o desarrollador de aplicaciones.

2. El **sistema de información** (hardware, redes propias, software básico, aplicaciones)

3. La propia **información**

4. Las **funcionalidades de la organización** que justifican y dan finalidad a la existencia de los Sistemas de Información, incluido el personal usuario o los objetivos propuestos por la dirección.

5. **Otros Activos** (por ejemplo la credibilidad de una persona jurídica o física, su intimidad, la imagen ...).

Un proyecto de seguridad articula los 5 tipos o niveles como 'capas' de Activos desde el punto de vista de las cadenas potenciales de fallos 'verticales' entre dichas capas. Así, fallos en Activos del Entorno (1) provocarían otros fallos en el Sistema de Información (2); éstos inciden en fallos de la Información (3), que soporta las funcionalidades de la organización (4) y ésas condicionan los otros activos (5). (Guía de Aproximación a la Seguridad de los Sistemas de Información, de MAGERIT, Pág. 17).

Metodología de trabajo:

Para elaborar la siguiente metodología he tomado como referencia las consideraciones sobre la información[11] y los aspectos referidos para asegurar la misma. El *Mapa de Seguridad* [12] que muestra de forma gráfica los aspectos involucrados a la hora de considerar un estudio sobre la seguridad de la información, y los ítems enumerados en *Aspectos de Seguridad Informática* [13] determinan el ambiente sobre el cual realizar un análisis de riesgos.

Para éste análisis he considerado aspectos metodológicos orientados al *Análisis de Riesgo* sugeridos en la "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información" (MAGERIT)[14].

Y, para captar el punto de vista de personas clave y poder sistematizar la información desde la tecnología de la información, he tomado como modelo las encuestas sugeridas por OCTAVE[15]; tanto para el personal en general como para el personal de Tecnología Informática.

La metodología de evaluación que se propone en la norma IRAM 17799 (traducción de la ISO/IEC 17799:2000) orientada a *Mejores Prácticas*, está en el espíritu de todo el relevamiento y posterior análisis.

[11] Marco Referencial. págs. 13 y 17
[12] Marco Referencial. págs. 21 y 22
[13] Marco Referencial. págs. 18 a 20
[14] Marco Referencial. págs. 31 a 32
[15] OCTAVE[SM] Method Implementation Guide Version 2.0, Carnegie Mellon – Software Engineering Institute, Pittsburgh, PA 15213-3890, http://www.cert.org/octave/ - septiembre de 2004

Esquemáticamente, la metodología a seguir es la siguiente:

• **Identificar activos** importantes relacionados con la información.

Mediante la orientación de las guías MAGERIT y los modelos de encuestas propuestos por OCTAVE, identificando las amenazas para cada activo y buscando vulnerabilidades de los mismos.

• Realizar, con la información recolectada, un **análisis de riesgo** de los activos informáticos.

• Identificar aquellos activos con mayor riesgo.

• Implementar controles concretos para reducir el nivel de riesgo de dichos activos.

Proponiendo **políticas de seguridad** que enmarquen las acciones a tomar.

Aplicando controles para ajustar los activos a las políticas.

Definiendo **planes de contingencias**.

Con esta metodología pretendo un acercamiento a la realidad de la problemática de la Seguridad Informática en la planta industrial de Arcor en Colonia Caroya.

Relevamiento

Información sobre la Planta Industrial

ARCOR S.A.I.C. es un Grupo Empresario argentino fundado en 1951

Actualmente focalizado en los negocios de golosinas, chocolates, alimento y packaging, cuenta con treinta y siete plantas productivas en Argentina, Brasil, Uruguay, Paraguay, Perú y Chile.

Para el desarrollo del trabajo he seleccionado la Planta de Chocolates, cita en Colonia Caroya Ruta 9 Km. 750. Esta fábrica es parte del negocio de Chocolates del grupo empresario ARCOR S.A.I.C.

Legajo técnico:

Distancia a la ciudad de Córdoba: 50 Km.
Superficie del terreno: 90.000 m^2.
Superficie cubierta total: 30.000 m^2.
Superficie de planta de producción: 23.000 m^2.
Superficie depósito de expedición: 5.000 m^2
Altura del depósito: 14 m.
Superficie de planta de Servicios Centrales: 2.000 m^2
Inicio de la construcción: Mayo de 1992
Puesta en marcha de la primera línea de producción (Bon o Bon): Mayo de 1993.
Puesta en marcha total: Mayo de 1994.

a) Un poco de historia:

ARCOR se fundó en 1951, con el propósito de fabricar caramelos, pero para contar la trayectoria de la empresa hay que remontarse a 1924. Fue ese año cuando Amos Pagani, un joven inmigrante italiano, decide radicarse en Arroyito, un pequeño pueblo argentino de la Provincia de Córdoba, para instalar una panadería.

En 1928 nace el segundo de los cinco hijos de Amos: Fulvio Salvador.

Él fue quien plantaría, años más tarde, la semilla de una gran empresa al proponer la idea de montar una fábrica de caramelos a un grupo de emprendedores pioneros, entre los que se encontraban sus hermanos Renzo y Elio; los hermanos Modesto, Pablo y Vicente Maranzana; Mario Seveso y Enrique Brizio.

En 1951 se desarrollan las obras de construcción de la primera fábrica.

El 5 de julio, finalmente, se inaugura la flamante planta y se inicia la producción.

En 1958, ARCOR ya había alcanzado los 600.000 kilos diarios de golosinas. Por entonces, había dejado de ser exclusivamente una fábrica de caramelos, a partir de la incursión en distintas actividades industriales. Actividades que tenían un objetivo claro: auto abastecerse de algunos insumos básicos con el fin de alcanzar la mejor calidad y el mejor precio.

En la década del '70 –y ante la realidad de una economía cerrada en la que era muy difícil conseguir insumos a precios competitivos- Arcor comienza a construir plantas que van satisfaciendo las diversas necesidades de la empresa, desde las materias primas hasta los envases, pasando incluso por la energía.

Así, Arcor inaugura en 1970 una planta en Tucumán; en 1972, una en San Rafael (Mendoza); en 1975, en Villa del Totoral (Córdoba); en 1978, en San Pedro (Buenos Aires); en 1979, nuevamente en Villa del Totoral; y en 1980, en Paraná (Entre Ríos). Para estos años, ARCOR se había transformado en un vasto complejo industrial, marcando el camino entre las empresas de su país. No obstante, la compañía continuaría creciendo tanto en la Argentina como en distintos países de la región. En 1976 se radica en Paraguay, en 1979 en Uruguay, en 1981 en Brasil y en 1989 en Chile.

Como se ve, ARCOR había comprendido tempranamente el valor de la integración latinoamericana y el potencial de un gran mercado común en la región, creando "su propio Mercosur" mucho antes de que la palabra misma existiera.

La vocación latinoamericanista de la empresa llevó a Arcor a crear su propio Mercosur una década antes de la firma del Tratado de Asunción.

En 1990, la empresa es sacudida por un doloroso acontecimiento. En plena madurez vital, un accidente termina con la vida de Don Fulvio Salvador Pagani, el mentor de una obra tan vasta como creativa. Surge así un nuevo desafío para la gente de ARCOR: tomar la posta y continuar la línea trazada por su conductor.

Hugo Enrique D'Alessandro, uno de sus actuales Directores, asume la Presidencia e inaugura un nuevo ciclo de concreciones, tomando como marco de acción un legado que el fundador había presentado 22 días antes de su desaparición: la nueva estructura organizativa de la empresa.

En este período, se levanta la Planta Modelo de chocolates de Colonia Caroya, la entonces más grande y evolucionada de Latinoamérica; se construye el gasoducto Pilar-Arroyito para abastecer a la empresa de un elemento vital y se adquiere Águila Saint, una de las más tradicionales y prestigiosas empresas chocolateras argentinas.

En el plano social, la empresa acentúa su presencia. En 1991 nace la Fundación ARCOR, con el objetivo de aportar soluciones en materia de salud, cultura y educación pública, apuntando a concretizar el anhelo de la empresa de contribuir a una mejor calidad de vida para la población.

En 1993, asume la Presidencia de ARCOR el Contador Luis Alejandro Pagani, hijo mayor de Don Fulvio. ARCOR toma entonces un renovado impulso, que la proyecta definitivamente hacia el mundo. Para ello, la empresa lleva adelante un profundo proceso de transformación de su management, alcanzando un alto nivel de profesionalismo, condición indispensable para adecuarse rápida y eficazmente a los nuevos escenarios económicos locales e internacionales. La competencia en la región se intensifica, producto de la entrada al juego de otras empresas multinacionales.

Bajo la conducción de Luis Pagani, ARCOR adquiere Noel, otra reconocida marca de alimentos y golosinas, con más de un siglo de prestigio. Se inaugura en Salto, Provincia de Buenos Aires, la planta de galletitas más evolucionada de la Argentina, dotada de los últimos avances tecnológicos en la materia y construida en un tiempo récord de apenas un año. Se

construye una nueva planta para la producción de cajas de cartón corrugado en Luján, Provincia de Buenos Aires. Esta planta ayudaría a consolidar el liderazgo nacional de Cartocor, una de las empresas integrantes del Grupo Arcor. Continuando con su fuerte expansión en Latinoamérica, Arcor desembarca en 1996 en Perú, construyendo una importante planta productora de caramelos para estar cada vez más cerca de los consumidores latinoamericanos.

En 1997, y para celebrar la acción desarrollada hasta entonces, la empresa inaugura el MUSEO ARCOR, una iniciativa cuyo principal objetivo es compartir retazos de su historia con la gente. En 1998, el Grupo Arcor concreta una de las operaciones más importantes de su vida empresaria. Adquiere la empresa chilena Dos en Uno, líder en golosinas y chocolates de su país y con una extensa penetración en la región. Esta compra afianza a Arcor en los países del Pacto Andino y le permite entablar mejores relaciones comerciales con los mercados del NAFTA. Un año más tarde, en 1999, otro hito espectacular: Arcor instala en Brasil la más avanzada fábrica de chocolates de la región, que cuenta con el mayor centro de distribución de productos del país. Un emprendimiento que ubica a la empresa a la vanguardia tecnológica y productiva en el continente y que le permite consolidarse en el sumamente atractivo mercado latinoamericano.

La extraordinaria planta de Bragança Paulista, en Brasil, le permite a Arcor apuntalar su visión de convertirse en la empresa de golosinas y chocolates número uno de Latinoamérica. Este vigoroso impulso ha llevado a Arcor a convertirse en una de las "multilatinas" más importantes de la región y en un ejemplo exitoso de expansión internacional. En la actualidad, el Grupo lidera la mayoría de las categorías donde participa con sus más de 1500 productos. Entre sus récords más recientes, sobresalen los siguientes: Arcor es el primer productor mundial de caramelos, líder en la fabricación de chocolates en Latinoamérica y el principal exportador de golosinas de Argentina y del Mercosur.

Para reflejar cabalmente estos logros y su dimensión empresaria global, en 1999 el Grupo Arcor renueva su simbología, creando una identidad visual altamente innovadora.

Ya en pleno siglo XXI, y con medio siglo de vida cumplido, Arcor sigue generando nuevos proyectos, apuntando siempre al mismo objetivo: "darle sabor" –como dice su slogan- a los

consumidores de todo el mundo. De un grupo de pioneros a un grupo multinacional líder en Latinoamérica. Una frase que sintetiza la historia de Arcor y que le sirve de carta de presentación en todos los rincones del planeta.

b) El Negocio Chocolates del Grupo ARCOR

A partir del año 1990 se verificó en Argentina un crecimiento sostenido en las ventas de golosinas a base de chocolates; fue entonces que la empresa ARCOR decidió ampliar la capacidad de producción en las plantas de Arroyito (Córdoba) y Misky (Tucumán).

La creciente y cada vez más diversificada demanda - especialmente en los segmentos de chocolates relleno y confitados, llevó al estudio de diversas alternativas, concluyendo que la producción de todos los productos que involucren chocolate debería centralizarse en una sola planta.

Es así como en Abril de 1994 se inaugura la planta de chocolates de Colonia Caroya, donde se comenzó elaborando setenta productos.

Con un volumen de producción de aproximadamente 150 toneladas diarias, se estimó que un 65% del total de ventas de chocolates del grupo ARCOR provendría de esta planta.

Fechas principales relacionadas con la Planta de Chocolates de Colonia Caroya:

1994	Puesta en marcha de la fábrica de chocolates de Colonia Caroya
1996	Certificación de normas ISO 9001, planta de chocolates Colonia Caroya.
1999	Inicio de TPM.
1999	Certificación de nueva versión de ISO. 9001
2000	Primera Expansión de TPM a toda la planta.
2003	Certificación de HACCP.
2005	Aprobación de preauditoría para el premio a la excelencia de TPM

c) Áreas de la planta:

La Planta de Chocolates de Colonia Caroya está conformada por las siguientes áreas:

?? **Depósito de Insumos.** Dentro de los cuales se consideran:
- Materias Primas.
- Materiales de empacamiento/envoltura.

?? **Pañol.** Depósito de:
- Repuestos e insumos mecánicos.
- Repuestos e insumos eléctricos.
- Repuestos e insumos de consumo para Servicios (agua caliente y fría, aire comprimido, etc.)
- Stock de elementos y productos de limpieza y químicos de uso en planta (accesorios reparaciones y otros).
- Insumos de recambio para mantenimiento edilicio.
- Generales: bolsas plásticas, contenedores, elementos de seguridad (zapatos, tapones auditivos, ropa, etc.).

?? **Talleres.** Comprende:
- Mecánicos.
- Eléctrico.
- Servicios Centrales.
- Contratistas / externos: en localizaciones que van desde exterior a dentro de planta.

?? **Producción.** Dentro de la que podemos identificar cuatro sectores claramente diferentes:
- Elaboración de Pastas y Rellenos.
- Fabricación de Productos Bañados: bombones y alfajores.
- Fabricación de Productos Moldeados: tabletas con y sin agregados. Incluye figuras huecas (huevos y otros).
- Fabricación de Productos Confitados.

?? **Oficinas Administrativas y de Soporte a la Producción.** Donde se incluyen además de las áreas puras de administración contable, los departamentos de:
   - Desarrollo.
   - Compras.
   - Sistemas.
   - M.A.H.P.I.
   - R.R.H.H.

?? **Laboratorio y Planta Piloto.** Donde se realizan ensayos sobre insumos o materias primas, materiales de empacamiento y producto terminado contando con secciones:
   - Fisicoquímica.
   - Microbiológica.
   - Empaque y maquinaria en pequeña escala para producciones reducidas de los productos elaborados en la planta.

?? **Expedición o Depósito de Producto Terminado.** Que a su vez es centro de Distribución por lo que almacena también productos producidos en otras plantas de la compañía, realizando despachos de mercadería únicamente al por mayor (camiones refrigerados).

d) Procesos de elaboración:

El proceso de ELABORACIÓN DE CHOCOLATE Y PRODUCTOS DE Y CON CHOCOLATE puede sintéticamente presentarse como la sucesión de las siguientes etapas:

✍✍Elaboración de Pastas: consiste en la incorporación de las materias primas, que incluyen:

- azúcar
- aceite/manteca
- leche entera o descremada
- cacao en la modalidad de licor o polvo
- e ingredientes menores tales como: sal, esencias, monoglicéridos, fosfátidos, etc;

a MEZCLADOR (fase seca), su pasaje por PREREFINADO y REFINADO, con la consiguiente disminución del tamaño de partículas principalmente de azúcar y la homogenización de la suspensión de partículas en fase grasa, TRANSPORTE (cintas de conducción) a CONCA, equipo clave del proceso donde tiene lugar el mayor trabajo mecánico, homogeneización, pérdida de volátiles y disminución de contenido de agua, ADICIÓN DE INGREDIENTES MENORES en fase final, tales como lecitina, sabores y resto de grasa/aceite/manteca.

✍✍Almacenamiento en tanques madres y Pulmones de línea, de distintas capacidades.

✍✍Moldeado: que básicamente consiste en la producción de tabletas, figuras huecas y rellenas, con consumo de las pastas elaboradas en la etapa anterior.

✍✍Bañados: que básicamente consiste en el bañado con consumo de las pastas elaboradas para tal fin en la etapa anterior, para la producción de bombones, alfajores y obleas. En estos casos, otros semielaborados son fabricados como parte del producto. Entre ellos: galletas y obleas.

e) Actividades relacionadas con la información:

En todas las áreas mencionadas arriba hay tareas de registro, informes y análisis de la información por medios electrónicos que soportan los procesos productivos y sirven para la toma de decisiones. Se pueden relacionar los diferentes ítems con su correlativo en el organigrama funcional de la página 52.

La siguiente lista fue tomada textualmente de las encuestas realizadas a los usuarios:

?? **Ingenieros de procesos:**

*seguimiento de prototipos;

*seguimiento de proyectos;

*análisis de indicadores y pérdidas;

*análisis de información de gestión industrial (JDEwards);

*consultas de SPAC (sistema de control de calidad).

?? **Control de producción:**

*One-World (JDEwards, sistema de gestión industrial);

*Carh (gestión de las personas: turnos, autorización de horas extras, etc.);

*Correo electrónico;

*Sistema de rendición de cuentas;

*Sistema de seguimiento de indicadores industriales;

*Sistema de mantenimiento mecánico;

*Planillas electrónicas (Tablero de comando; Indisponibilidad);

*Costos;

*Análisis varios de control de producción; etc.

?? **Medio Ambiente, Higiene y Protección Industrial:**

*Registro y estadísticas de accidentes;

*Registro y estadísticas de control de plagas;

*Registro y estadísticas de Tarjetas de Incidentes;

*Tratamiento sistemático de problemas;

*Auditorias;

*Legislación aplicable;

*Registro y estadísticas de residuos sólidos;

*Registro y estadísticas de efluentes líquidos;

*Registro de mediciones de higiene.

*Registro en hojas de revisión de elementos de seguridad;

*Procedimientos;

*Material de capacitaciones en seguridad;

*Planillas de permisos de trabajo;

*Planillas de stock de indumentaria del personal;

*Registros de limpieza;

*Registros de aparatos sometidos a presión;

*Registros de emanaciones gaseosas.

?? **Administración de Mantenimiento y Oficina Técnica:**

*Administración de recursos (materiales y mano de obra);

*Realización/impresión de reportes para mantenimiento preventivo;

*Manejo de información técnica (planos, manuales, instructivos, etc.)

?? **Administración de materiales productivos:**

*Se verifican necesidades de Materiales Productivos, sus consumos. Se pasan órdenes de compra por correo y luego se activan telefónicamente.

?? **Instructores del SGI.:**

*Pedidos de compras de materiales auxiliares;

*Pedidos al almacén;

*Excel, PowerPoint, Word, Paint, Editor Fotográfico, AutoCad;

*Internet;

*Correo electrónico;

*Sistema de rendición de cuentas;

*Módulo de tarjetas (administración de tarjetas de fallas o mejoras en equipos o procesos productivos);

*Scanneos, Impresiones color y b/n;

*Carh (gestión de las personas: turnos, autorización de horas extras, etc.);

*People Soft (Registro y administración de capacitaciones del personal).

?? **Gestión de Calidad:**

*Inspección (aprobación / rechazo) de insumos (materia prima y materiales de empaque);

*Compra de insumos de laboratorio (reactivos, descartables, etc.), librería (stickers de identificación de estado), etc.;

*Control de proceso (estadísticas de variables y atributos);

*Control de producto;

*Cálculo de Indicadores (reclamos, producto No conforme, índices de calidad);

*Check de cumplimiento de condiciones en base a especificaciones.

?? **Gerente corporativo de Gestión de Calidad:**

***Correo electrónico;

*Documentos en Word, Excel, PowerPoint (creación y almacenamiento);

*Aprobación de compras;

*Consultas de Internet;

*Consulta / búsqueda de información en Servidores.

?? **Compras:**

*Procesamiento de datos para gestión de compras;

*Comunicaciones internas y con proveedores vía correo electrónico;

*Búsqueda de información en Internet;

*Sistema para el Seguimiento del mercado del Cacao;

*Emisión de pedidos de compra (JDEwards);

*Seguimiento de evolución de indicadores;

*Elaboración de estadísticas relativas a compras.

?? **Jefe del Centro de Distribución:**

*Control de Warehousing en todo el Centro de Distribución (Ingreso y egreso de mercadería, confirmación de productos terminados en almacenamiento. Confirmación de pedidos, créditos, devoluciones prebalanceo y balanceo de carga. Facturación.

?? **Jefe de Investigación y Desarrollo:**

*Administración de Prototipos;

*Confección de Especificaciones;

*Seguimiento de Proyectos;

*Inscripción Bromatológica.

f) Sistema de Gestión Integral; marco general de trabajo en el establecimiento industrial:

Es de especial importancia ubicar al lector en cómo está estructurado todo el accionar de la empresa alrededor de un sistema de gestión llamado: Sistema de Gestión Integral (SGI).

Éste está fuertemente enfocado en la idea de alcanzar la autogestión o autonomía de cada colaborador (así llamamos a cada empleado en la fábrica) en su puesto de trabajo.

Se jerarquizan los puestos, se evalúan las habilidades y la capacitación necesaria para cada puesto generando matrices complejas. Si bien son difíciles de leer, observando con atención y con un poco de orientación se puede distinguir cada línea de producción con sus colaboradores más operativos; pasando por quienes controlan los procesos y la calidad; por quienes supervisan y gerencian las actividades. Y para cada uno se ven sus necesidades cubiertas o faltantes para el puesto.

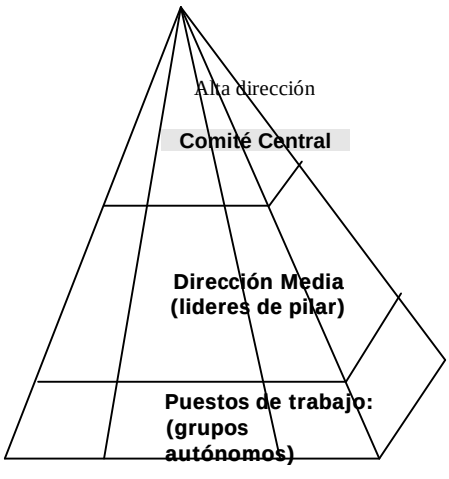
Las personas se reúnen en grupos autónomos en los cuales se gestionan, conversan y discuten los problemas particulares de su sector.

A la vez participan en pilares del sistema: Seguridad, Calidad, Gestión Temprana; Mantenimiento Productivo; Mantenimiento Autónomo; Capacitación; Administración y Mejora Continua.

Los líderes de cada pilar se reúnen semanalmente en el Comité Central donde se evalúan los inconvenientes del proceso y las sugerencias de mejoras, entre otras cosas.

Así se forma una red de grupos intercomunicados que a simple vista se descubre como muy interesante, creativo, integrador y formativo en la participación y responsabilidades colectivas.

Cada grupo y pilar tienen objetivos claros y medibles puestos por ellos mismos y coordinados por el comité central. Así mismo se evalúa la gestión completa del sistema con auditores de un comité general del grupo Arcor. Todo es seguido y evaluado por un consultor externo de empresas.



Algo más a cerca de los grupos autónomos:

El SGI combina los objetivos de la dirección que fluyen de arriba - abajo con las actividades de los grupos autónomos (comunicación vertical ascendente y horizontal). A la vez la integración en pilares nos acerca modelos de comunicación transversal.

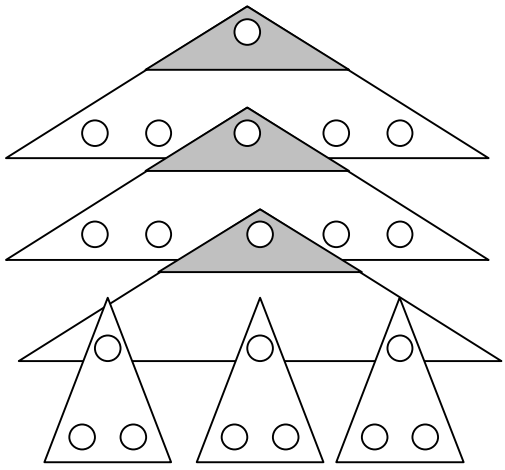
La figura que sigue ilustra el mecanismo de funcionamiento, basada en la filosofía del SGI.

El éxito o el fracaso del SGI depende en alto grado del compromiso de la dirección. Los objetivos se comunican con amplitud a cada empleado en todos los niveles de la organización. Cada grupo autónomo debe establecer sus propios objetivos.

Aunque los pequeños grupos SGI operan autónomamente dentro de sus términos de referencia, siempre permanecen dentro de las directrices de la organización general.

Estructura solapadas de los grupos de SGI:

Las actividades de los grupos SGI son parte integral de las actividades formales de la organización. Los grupos SGI abarcan a toda la jerarquía de la organización desde la alta dirección, a la dirección media y los operarios.



Estructura solapada

Esta integración abajo - arriba se logra solapando los pequeños grupos (ver la figura que sigue): Los lideres de grupos de nivel son miembros de los grupos del siguiente nivel más elevado. De este modo, se conectan formando una pirámide integral. El pequeño grupo de lo alto de la pirámide esta integrado por directivos de la empresa, y esta liderado por el de mayor jerarquía de la planta. Siguen hacia abajo los pequeños grupos de los jefes de sección liderados respectivamente por directivos de la empresa seguidos por los grupos de subjefes de secciones. La base de la pirámide consiste en operarios liderados por sus supervisores o líderes de línea.

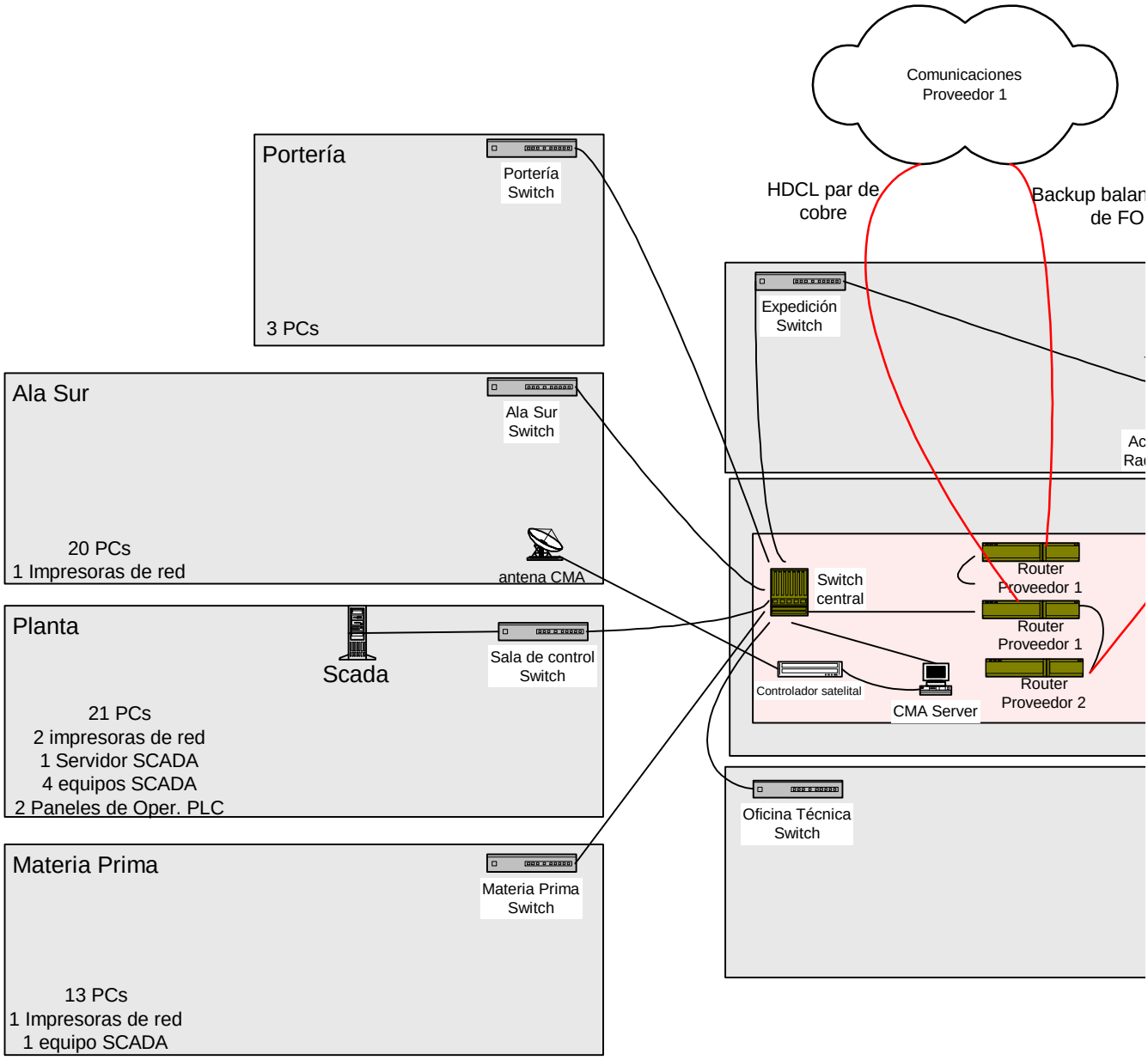
Todo esto actúa como correa de transmisión, facilitando la comunicación en forma horizontal, vertical y transversal (integrando los diferentes departamentos).

Relevamiento esquemático:

En las próximas páginas se presenta un esquema de toda la red informática en Arcor - Colonia Caroya, mediante el cual se puede dimensionar el sitio.

Luego se incluye un relevamiento de todos los puestos de trabajo (evitando consignar nombres de usuarios). Éste relevamiento es un indicador del nivel de identificación física de los activos de la red y cada puesto de trabajo en la misma.

Además se agrega un organigrama funcional.


Comunicaciones
Proveedor 1
HDCL par de cobre
Backup balan
de FO
Portería
Portería
Switch
3 PCs
Ala Sur
Ala Sur
Switch
20 PCs
1 Impresoras de red
antena CMA
Planta
Scada
Sala de control
Switch
21 PCs
2 impresoras de red
1 Servidor SCADA
4 equipos SCADA
2 Paneles de Oper. PLC
Materia Prima
Materia Prima
Switch
13 PCs
1 Impresoras de red
1 equipo SCADA
Expedición
Switch
Switch
central
Router
Proveedor 1
Router
Proveedor 1
Router
Proveedor 2
Controlador satelital
CMA Server
Oficina Técnica
Switch

Cómputos (Ala Norte)

Pachera		Switch
1	Puesto 001	37
2	Libre	10
3	Puesto 002	51
4	Libre	-
5	Puesto 003	54
6	Puesto 004	6
7	Puesto 005	7
8	Libre	8
9	Puesto 006	9
10	Libre	-
11	Imp. de red 01	11
12	Puesto 007	12
13	Puesto 008	13
14	Puesto 009	14
15	Imp. de red 02	15
16	Puesto 010	16
17	Puesto 011	17
18	Puesto 012	18
19	Puesto 013	19
20	Puesto 014	20
21	Puesto 015	21
22	Libre	22
23	Puesto 016	23
24	Puesto 017	24

Pachera B		
25	Puesto 018	25
26	Puesto 019	26
27	Libre	-
28	Libre	28
29	Libre	29
30	Puesto 020	30
31	Puesto 021	31
32	Puesto 022	32
33	Libre	38
34	Puesto 023	34
35	Puesto 024	35
36	Puesto 025	36
37	Libre	-
38	Libre	-
39	Libre	39
40	Libre	40
41	Puesto 026	1
42	Libre	-
43 S1	Servidor 01	3
44 S2	Servidor 02	4
45 S3	Servidor 03	5
46 S4		
47 S5	Servidor 04	33
48 S6	Servidor 06	27

Expedición

Pachera A		Switch
1	Libre	
2	Puesto 030	
3	Puesto 031	
4	Imp. de red 04	
5	Puesto 032	
6	Imp. de red 05	
7	Puesto 033	
8	Puesto 034	
9	Puesto 035	
10	Puesto 036	
11	Puesto 037	
12	Puesto 038	
13	Imp. remota 1	
14	Imp. remota 2	
15	Libre	
16	Puesto 039	
17	Libre	
18	Puesto 040	
19	Puesto 041	
20	Libre	
21	Puesto 042	
22	Puesto 043	
23	Puesto 044	
24	Libre	

Pachera B		
1	Puesto 045	
2	Puesto 046	
3	Puesto 047	
4	Libre	
5		
6	Puesto 048	
7		
8		
9		
10	Puesto 049	
11	Imp. remota 3	
12	Puesto 050	
13	Puesto 051	
14	Imp. de red 06	
15	Imp. de red 07	
16	Radio Fr. 1	
17	Radio Fr. 2	
18	Radio Fr. 3	
19		
20		
21		
22		
23		
24		

Planta

Pachera A		Switch
1	Puesto 064	10
2	Puesto 065	2
3	Puesto 066	3
4	Puesto 067	4
5	Puesto 068	5
6	Puesto 069	6
7	Puesto 070	13
8	Puesto 071	8
9	Imp. de red 09	9
10	Puesto 072	23
11	Puesto 073	11
12	Puesto 074	12
13	Puesto 075	7
14	Puesto 076	14
15	Servidor 08	15
16	SCADA 2	16
17	Puesto 077	17
18	SCADA 3	18
19	Puesto 078	19
20	Puesto 079	20
21	Puesto 080	21
22	SCADA 4	22
23	SCADA 5	1
24		Hub de SCAD

Pachera B		
1	Puesto 081	
2	Puesto 082	
3		
4		
5		
6		
7		
8		
9	Panel Oper. PLC 1	
10	Puesto 083	23
11	Panel Oper. PLC 2	40
12	Imp. de red 10	36
13		
14		
15		
16		
17		
18		
19		
20		
21	Puesto 084	45
22		
23		
24		

Pachera C		
49 S7	Servidor 07	59
50 S8	Libre	2
51	Libre	-
52	Puesto 027	52
53	Puesto 028	53
54	Libre	-
55	Puesto 029	55
56	Libre	56
57	Imp. de red 03	57
58	Libre	58
59	Servidor 05	-
60		60 - Router
61		-
62		-
63		-
64		-
65		-
66		-
67		-
68		-
69		-
70		-
71		-
72		-

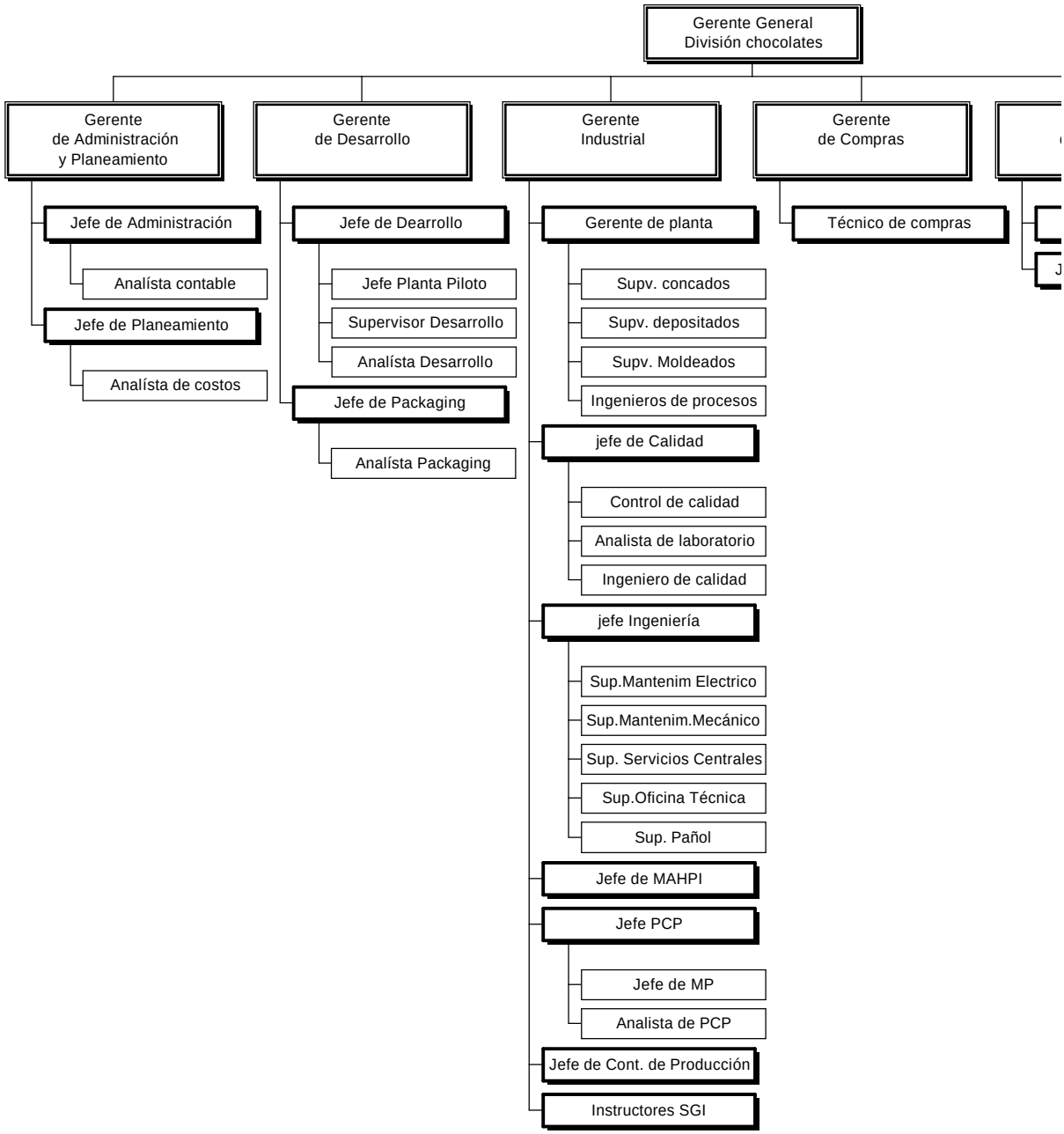
Materia Prima

Pachera		switch
1	Puesto 052	1
2	Puesto 053	20 (10 Mb)
3	Puesto 054	3
4	Puesto 055	4
5	Puesto 056	5
6	Libre	6
7	Puesto 057	7
8	Puesto 058	8
9	Puesto 059	17 (10 Mb)
10	SCADA 1	10
11	Puesto 060	11
12	Imp. de red 08	12
13	Puesto 061	13
14	Puesto 062	14
15	Puesto 063	15
16		
17		
18		
19		
20		
21		
22		
23		
24		

Ala Sur

Pachera		switch
1	Puesto 085	
2	Puesto 086	
3	Puesto 087	
4	Puesto 088	
5	Puesto 089	
6	Puesto 090	
7	Libre	
8	Puesto 091	100
9	Puesto 092	
10	Puesto 093	
11	Puesto 094	
12	Puesto 095	
13	Puesto 096	
14	Puesto 097	
15	Libre	
16	Puesto 098	
17	Puesto 099	
18	Puesto 100	
19	Puesto 101	
20	Libre	
21	Puesto 102	
22	Puesto 103	
23	Puesto 104	
24	Imp. De red 11	

ARCO SAIC - División Chocolates (Organigrama FUNCIONAL)



Evaluación (descriptiva) de la situación.

Evaluación, en cuanto a la Seguridad Informática, siguiendo la encuesta sugerida por OCTAVE para el personal de tecnología informática.

Siguiendo pautas de la IRAM 17799 se enumeran a continuación aspectos relacionados con la información en su disponibilidad, confidencialidad e integridad.
Luego se distinguirán los activos importantes para estudiar su criticidad, revisando sus vulnerabilidades y amenazas fijando métricas según las guías de análisis de MAGERIT.

En toda la información presentada se evitará especificar datos sensibles, técnicos, nombres de equipos (sí funciones de los servidores por ejemplo) o nombres de empleados, sistemas operativos o las versiones o actualizaciones de los mismos. Tampoco se brindará la topología de red en detalle y no se dará ningún número de dirección de equipo.

Seguridad física:

Todos los aspectos enumerados serán evaluados y se les dará un nivel de criticidad para poder evaluar la urgencia ante la necesidad de tomar una medida preventiva.
Perímetro de seguridad:
Puertas, ventanas, cerraduras, alarmas.
Controles de acceso físico: Visitantes. Identificación visible.
Protección de oficinas, recintos e instalaciones.

La planta industrial tiene un servicio de Guardia tercerizado que debe responder a la oficina de Recursos Humanos.
El personal de guardia debe hacer rondas periódicas de control por todo el recinto industria.
Lo hacen registrando, mediante un sistema informatizado, la hora en que pasan por ciertos puntos críticos preestablecidos.
Entre los varios controles deben hacer a las personas que ingresan tienen la responsabilidad de registrar la entrega de llaves de cada oficina, sala o sector.
Deben entregar todos los días las planillas de ingresos de visitas, contratistas y del personal jerárquico.

Para una apoyo a estas funciones existe un contrato con Gendarmería Nacional en el que se prescribe que dos personas de la fuerza deben controlar el perímetro de la planta.

En portería se entrega a todo visitante un cartel de visita que debe ser llevado a la vista. Toda persona visitada debe ir a buscar al visitante y debe acompañarla hacia la guardia cuando se retira. También deben firmarle un pasaporte de control de visitas.

Los contratistas tienen una carpeta en la oficina de RRHH por la que se les controla la vinculación efectiva a la empresa con la que trabajan; se controlan los aportes previsionales; el seguro de ART y los aportes a la AFIP. Esta información debe ser actualizada mensualmente, caso contrario se les prohíbe el ingreso al establecimiento industrial.
Todos estos aspectos se pueden ver en detalle en archivos físicos en RRHH:
"Procedimientos de visitas Guiadas a Planta"
"Requisitos para ingreso de Contratistas"
"Reconocimiento de propiedad y compromiso de confidencialidad en el manejo y conocimiento de información".
"Folleto de Normas para visitantes con acceso al Área de Producción".

Con respecto a la seguridad ante eventos existe una oficina de Medio Ambiente Higiene y Protección Industrial (MAHPI) que consta de dos personas.
Esta oficina mantiene todo un procedimiento de controles. En ellos se incluyen procedimientos de atención de alarmas contra incendios, con planes de evacuación organizados mediante brigadas de emergencia. Toda persona que tenga responsabilidades en estas brigadas está debidamente identificadas mediante un brazalete. Están en etapa de formación y están preparando planes de acción y evacuación con roles bien definidos.
También se encargan de la capacitación de toda persona que trabaje en la fábrica.
Existen pulsadores para activar alarmar y detectores de hubo en los sectores de mayor riesgos de incendios.
El área de MAHPI está constantemente auditada desde el Sistema de Gestión Integral SGI, ya mencionado en el relevamiento estructural de la planta.

Centro de cómputos:

En el centro de cómputos existen cuatro detectores de humo distribuidos uniformemente. Además hay dos matafuegos. Uno de dióxido de carbono (CO2) y otro de espuma (Halon) especial para equipos electrónicos. El personal de MAHPI, por medio de las brigadas contra incendios, los controlan mensualmente y se aseguran que se recarguen todos los años.
El personal de sistemas, como toda persona del establecimiento, ha realizado una jornada de capacitación teórico práctica para identificar y utilizar los diferentes tipos de matafuegos según el tipo de siniestro.
No hay protección especial contra el polvo, el agua o la humedad, salvo que el equipamiento está sobre mesas o en racks especialmente diseñados. La limpieza del sector se hace durante el día con supervisión del personal de sistemas.
La temperatura se controla mediante dos termómetros y existen dos extractores de aire en la parte superior de los tabiques divisorios. El aire frió se mantiene mediante circulación de agua fría a 5°C que mediante ventiladores y radiadores dispersa el aire frió en la sala. El agua fría como la circulación se controlan desde el área de Servicios Centrales. Existen procedimientos y controles monitorizados por el SGI para garantizar que el servicio sea permanente. Cabe aclarar que el agua fría también es indispensable para muchos sectores en las líneas de producción.

Protección eléctrica.

Existe UPS, tiene alarmas de cortes, se apagan automáticamente los equipos, se disparan alarmas, cada equipo tiene su térmica independiente.
La alimentación eléctrica se brinda desde un tablero central, cercano a la puerta del edificio. Sólo tienen acceso el personal de mantenimiento eléctrico y el de sistemas siguiendo el procedimiento de entrega de llaves del personal de guardia. Las llaves térmicas del tablero están bien identificadas.

En el centro de cómputos un pequeño tablero eléctrico distribuye la energía a dos UPS, de 1 y 6 Kva. respectivamente. Hay dos circuitos. Uno para los equipos más delicados con la protección de la UPS mayor. En ambos circuitos los equipos están sobre la misma línea sin tener llaves térmicas independientes. La autonomía de la UPS, verificada por el personal de sistemas, es de 45 a 60 minutos.

Se garantiza el suministro eléctrico mediante una subestación controlada por personal de mantenimiento eléctrico de la fábrica.
Es de notar que no existen interruptores ni luces de emergencia.

Control de acceso a personas no autorizadas:

El personal de seguridad de la fábrica tiene indicaciones claras por escrito a quién darle las llaves del centro de cómputos. Sin embargo no existe un procedimiento escrito guardado en un lugar accesible para actuar ante problemas importantes. Ante cortes del suministro no se disponen de procedimientos para saber qué hacer y a quién dirigirse. La experiencia indica que primero llaman al personal de mantenimiento eléctrico y en ocasiones recuerdan llamar al soporte informático.
No existe vigilancia de acceso ni monitoreo. Tampoco, por supuesto, un procedimiento escrito de monitoreo.

Ver aspectos sobre respaldos de información y procedimientos y cuidados de los medios de almacenamiento de los mismos abajo en el apartado: Backups

Equipos periféricos de comunicación:

Los diferentes switchs periféricos están en racks con acceso restringido pero no todos tiene cerradura con llave.
En cuanto a la protección eléctrica; están inventariados y bien identificados los tableros con las respectivas llaves térmicas; tienen estabilizadores individuales y el lugar es seguro y con acceso restringido.

Los equipos de comunicación principales están en el Centro de cómputos que tiene acceso restringido. La sala está en un ambiente controlado. El personal de seguridad tiene instrucciones claras y escritas sobre a quién y en qué circunstancias facilitar el acceso. Vale todo lo mencionado en el apartado Centro de Cómputos incluyendo lo referente a la protección eléctrica y el ambiente.

Estaciones de trabajo:

No se restringe masivamente el acceso a disqueteras, unidades de CD y módems. Sólo se hace en algunos sectores en los que los equipos se utilizan por muchas personas y están en áreas no bien vigiladas.

Los gabinetes no están protegidos contra sabotajes (de hecho ya hubo robos de discos, teclados y mouses). Hay sectores que en los fines de semana quedan muy solitarios y sin control de acceso. Esos equipos quedan muy desprotegidos y el intruso podría hacer su "trabajo" sin dificultad y sin ser visto. En oficinas de administración, desarrollo o control de producción (para nombrar algunas) los sectores quedan bajo llave o a cargo de algún responsable del sector o seguridad.

En cuanto a las protecciones contra robo, incendio, humo, agua, interferencia y las condiciones ambientales, son las mismas que rigen para el ambiente industrial dónde hay equipamientos y procesos probablemente más críticos que el cuidado de alguna de las estaciones de trabajo. El área de MAHPI está encargada de estos aspectos.

Mantenimiento de equipos. Contratos con proveedores de servicio:

Hay un contrato estricto de mantenimiento de equipos con una firma externa. Éste contrato incluye procedimientos, responsabilidades, tiempos establecidos para la puesta en funciones de equipos con desperfectos dependiendo de su criticidad. Se lleva un inventario de hardware en el que se consigna (de mutuo acuerdo) cuales equipos entran en régimen de críticos y cuáles no. También se establecen parámetros de ambiente hostil o no con lo cual se fija un régimen de control preventivo y limpieza periódico dependiendo del grado de hostilidad. También se ha fijado un régimen semanal de visitas para reparaciones y controles preventivos en el sitio. En el contrato también se establece que el contratista debe tener elementos de hardware para respaldar rápidamente alguno crítico que haya fallado (por ejemplo las impresoras de alto régimen en las oficinas de facturación).

Para los equipos con información sensible hay un procedimiento en que se consigan que la reparación debe ser in situ y en caso de no poderse se indica que se llevará el equipamiento sin la información.

En cuanto a la información de los equipos, está establecido que no se debe registrar localmente nada de criticidad. Cada usuario o grupo tiene asignado en los servidores un

lugar para ésta información. Los usuarios están (mayoritariamente) concientizados al respecto.

No hay políticas de equipos establecidas y se depende del criterio del soporte informático y de cada usuario para el resguardo y buen uso de los elementos de soporte informático.

En casi todos los equipos las personas no tienen restricciones: pueden instalar software; compartir impresoras o carpetas; leer y copiar CDs; etc.

Seguridad del equipamiento fuera del ámbito de la empresa:

Con respecto a los equipos móviles rigen las mismas consideraciones realizadas para los equipos fijos. Se le agrega que al ser transportables son factibles de robos, extravíos, roturas o usos indebidos no relacionados con el negocio.

Esta situación hace el cuidado de estos equipos sea considerablemente más crítico.

Baja segura o reutilización de equipamiento: Licencias. Datos:

El descarte de los equipamientos en desuso no está regido por ningún procedimiento. Se suelen donar los equipos, pero no se brindan con las respectivas licencias y la información se borra dependiendo del criterio del soporte informático.

Ingeniería social:

Específicamente no hay una política de control de accesos. Sí, hay procedimientos más o menos estrictos y que pretenden ajustarse a las normas antiterrorismo que Estados Unidos pretende de las empresas con las que comercializa.

Contratos de confidencialidad con el personal (en especial con el personal de Sistemas); con proveedores o terceros.

Se ha firmado un documento de confidencialidad con el personal de sistemas. Con el resto del personal solo es aconsejado, no es requisito de continuidad y permanencia en la empresa.

Con proveedores de sistemas existen contratos con los dos proveedores de servicios vinculados con la información: la empresa encargada del servicio técnico y la que mantiene los equipos de automatización del equipamiento de producción (equipos SCADA: Sistemas de Captura y Análisis de Datos.)

De hecho, toda entidad que pretenda brindar servicios a Arcor debe atenerse a ciertos procedimientos de seguridad y confidencialidad. En los anexos 5, 6 y 7 se puede ver un modelo de contrato de confidencialidad y una lista de requisitos y recomendaciones. Tanto la oficina de RRHH como de MAHPI velan para que estos aspectos sean cumplidos. El mismo sistema SGI audita estrictamente estos aspectos.

Políticas y Procedimientos:

Altas y bajas de personal. Administración de privilegios. Administración de contraseñas. Derechos de acceso. Controles de acceso a la red.

No hay políticas de RRHH para alta o bajas de personal. Sí hay procedimientos claros de altas pero no en lo referente a los sistemas informáticos. Tampoco hay políticas escritas de seguridad de equipos, usos de los medios electrónicos brindados, altas y bajas de usuarios. Existen procedimientos más o menos rigurosos de altas de usuarios, perfiles de seguridad y entornos de trabajo en determinados sistemas corporativos. (Ver procedimientos de manejo de la información clasificados según las áreas operativas de la fábrica en el relevamiento estructural.)

Capacitación y concientización sobre la problemática de seguridad informática.

Para toda persona que comienza a trabajar en este establecimiento industrial hay procedimientos bien claros para el ingreso: Capacitación requerida según el puesto; exámenes de salud rigurosos; se ofrecen cursos de inducción como "Buenas prácticas de manufacturas" y "Manejo de matafuegos".

Sin embargo no hay ninguna inducción al personal a cerca de la seguridad informática. Falta una adecuada sensibilización de los usuarios a cerca de los riesgos informáticos, ya sea por fraudes, ataques o por el manejo incorrecto del equipamiento informático al que accederá. Tampoco existen planes de capacitación – concientización al respecto. No se hace mención a la confiabilidad y confidencialidad de la información que manejarán.

Por lo tanto los usuarios dependen (ante sus dudas o inconvenientes) de sus propios esfuerzos o de la buena voluntad de comunicación del soporte responsable de sistemas.

Modo de destrucción de papelería importante. Certificación.

Si alguien considera que algún medio de almacenamiento o papelería es muy importante o confidencial pude solicitar al área de MAHPI la destrucción segura. Dicha área dispone de contactos con empresas del medio las cuales pueden decomisar, destruir y certificar materiales siguiendo la norma ISO 14.000 de Gestión Ambiental – Desarrollo Sostenido.

Con respecto al retiro de información de la planta (en medios de almacenamiento o papeles) no hay nada establecido. Cualquiera que no sea operario de planta pude salir sin ser requisado y llevar CD, carpetas con información etc.

El uso de las fotocopiadoras, impresoras y fax está únicamente restringido por el espacio físico. Las personas que pueden acceder al área no tienen mayor control que el de la imputación de las fotocopias que hagan a su centro de costos por medio de un código.

Plan de contingencias:

No hay planes de contingencia alguno. Sólo el personal de MAHPI tiene procedimientos de evacuación e incluso tienen previsto realizar simulacros de evacuación. Además, como ya se mencionó más arriba, se están formando y capacitando brigadas de seguridad.

Seguridad de Servidores y Estaciones de Trabajo:

Privilegios de login de usuarios de PC.

No está especificado ningún privilegio y los usuarios se loguean como administradores de su equipo. Sólo hay un estricto procedimiento para loguearse en equipos de automatización SCADA y en los servidores. Esto último está regido por Tecnología Informática desde su gerencia de Seguridad Informática.

Login de servidores.

Generalmente no hace falta que los servidores estén logueados, pero cuando se necesita, la sesión se toma como administrador del sistema. Esto depende únicamente del criterio del soporte funcional. Existen recomendaciones telefónicas o buenas prácticas obtenidas de Internet pero sobre todo se basa en la responsabilidad, profesionalidad y buen criterio del responsable de sistemas.

Procedimientos de configuraciones de seguridad en servidores:

Existe y está adecuadamente documentado por TI. Además existe un control de las actualizaciones de seguridad liderado por el Grupo de Seguridad Informática (GSI).

Procedimientos de configuraciones de seguridad para PC de usuarios.

No hay nada oficial que oriente la configuración de seguridad, sobre todo para los equipos con los nuevos SO que sí facilitan la configuración al respecto.

Tampoco hay algo preestablecido para el uso de unidades de CD o disquetes. Según el nivel de problemas del sector se restringen para evitar el mal uso. Pero nuevamente se deja a responsabilidad, buen criterio y profesionalismo del soporte informático local. Lo mismo se puede decir respecto de contraseñas de BIOS.

El uso de módems está estrictamente prohibidos pero no hay un documento que así los indique. No hay servicios de RAS, para acceso remoto se habilita al usuario solicitante mediante un procedimiento a seguir vía GSI.

Utilización de la red y recursos compartidos:

Que tipo de archivos se encuentras en las carpetas compartidas de los servidores

No existen políticas, ni recomendaciones de uso de los medios informáticos. Tampoco hay concientización ni capacitación para que cada nuevo usuario se pueda ubicar en el entorno de trabajo.

Los usuarios no tienen restricciones de compartir recursos. Sólo se restringe por sectores críticos o con problemas dependiendo del soporte local y no hay política o recomendación escrita alguna. De hecho se han encontrado en recursos de red archivos de muy diferentes tipos con fines no productivos: música, videos, instaladores, etc. También se han encontrado papeles impresos que por su contenido son personales o al menos no fueron impresos con fines productivos.

Correo electrónico:

Protección contra virus, spam e información que sale de la empresa.

El personal no está concientizado y no tiene un procedimiento o sugerencias de cómo actuar o a quién dirigirse en caso de inconvenientes. Se han enviado correos con advertencias y sugerencias pero no han tenido el efecto deseado; las personas vuelven a preguntar una y otra vez sobre qué hacer ante determinados mail y se sorprenden de recibir mail de todo tipo con originadores y destinatarios desconocidos.

Las personas puede recibir y enviar mails desde y hacia fuera de la empresa.

Hay reglas de filtrado de correos para controlar los spam y virus informáticos que ingresan por el servidor central de correo. (Todos los mensajes que entran y salen de Arcor pasan por dicho servidor.)

El servidor de correo, junto con otros servidores de seguridad, el proxy de Internet, el servidor web o VPN están protegidos en una subred DMZ la cual en su conjunto actúa como Firewall. Todos estos equipamientos están bajo control de GSI.

Antivirus:

Las estaciones de trabajo y servidores tienen instalado un antivirus común a todo el Grupo Arcor.

Se posee una suscripción con una firma del medio que ofrece servicios de seguridad mediante un software antivirus. La misma libera cotidianamente en su sitio web actualizaciones, herramientas correctoras y advertencias.

La actualización suele ser semanal. Cuando se difunden nuevos virus o amenazas, el proveedor del producto, ofrece servicios adicionales.

Si bien la actualización de los servidores es automática, se depende del soporte informático local su para su monitoreo y efectiva actualización. Las estaciones de trabajo lo hacen mediante un comando en el logon script. Con este procedimiento se redujo el porcentaje de PCs desactualizadas a menos del 3% (en este sitio de Arcor). Éstos procedimientos están documentados mediante una base de datos de procedimientos y operaciones a la cual acceden todos los soportes informáticos. Para algunos casos falta detallar procedimientos de control y verificación.

No hay procedimientos de contingencias documentados ante ataques por virus.

Backups:

El procedimiento de realización de respaldos, que es automatizado, está correctamente documentado. Además el software es un producto del mercado y existe un contrato de soporte con el proveedor del mismo.

La información que se respalda es la de todos los archivos de usuarios almacenadas en los servidores, más los datos sensibles de los diferentes sistemas y las bases de datos.

Semanalmente también se respaldan los motores de bases de datos. Mensualmente se respalda la información de los equipos móviles de los usuarios jerárquicos.

El backup diario es realizado mediante el esquema Diferencial: Un backup completo por semana y los demás días diferencialmente salvando los archivos modificados desde el último backup completo.

No hay un método de verificación de backup documentado, periódico y controlado. La verificación se hace cotidianamente mediante la recuperación de información solicitada por los usuarios.
El almacenamiento de los medios de backup es seguro y con acceso restringido. No se hacen copias de las cintas. La grabación es encriptada por sesiones.
Las cintas se guardan en una caja fuerte inífuga con combinación.
Si bien el método de destrucción de cintas no está documentado, existen procedimientos regidos por MAHPI para hacerlo de forma segura y certificada.
No está establecido el tiempo de dar de baja a las cintas. Se realiza luego que hayan fallado.

Si bien hay conciencia de los usuarios de dónde guardar la documentación importante a fin de que sea respaldada, no es totalmente generalizada.

Identificación de Activos

Para la identificación de activos se han utilizado las Guías MAGERIT que, como ya se mencionó en el marco teórico, clasifican a los activos en 5 categorías:

1. El **entorno**
2. El **sistema de información** (hardware, redes propias, software básico, aplicaciones)
3. La propia **información**
4. Las **funcionalidades de la organización**
5. **Otros Activos**

1. Activos relacionados con el nivel del Entorno.

- **Equipamientos y suministros (energía, climatización, comunicaciones)**

Todo el equipamiento en el centro de cómputos (incluidos los servidores y equipos de comunicación) está asegurado mediante un sistema de alarmas contra incendio. El ambiente está climatizado por un sistema mantenido por el área de Servicios Centrales. Ésta área es de las más críticas del establecimiento industrial, porque mantienen la climatización para los productos terminados como el agua fría o caliente para todos los estados de producción. Esto garantiza que para el centro de cómputos no falte la refrigeración.
Se posee una UPS de 6 Kva. y otra de 1 Kva. con las que se garantiza la continuidad de las operaciones por una hora. En los sitios periféricos dentro del establecimiento no se poseen UPS pero sí se tiene la energía estabilizada para cada switch.
Para los diferentes equipos de PC en planta no se posee ninguna seguridad especial. Simplemente en algunos casos las PC están en gabinetes (Racks) pero no tienen llave. Se protegen así del ambiente.
En las oficinas de personal jerárquico se cuenta con cerraduras y control de la entrega de llaves por medio del personal de seguridad de la empresa.

El ambiente de operación también está controlado: durante todo el año se dispone de un clima adecuado para el personal. Esto está controlado por personal de MAHPI (Ver

relevamiento estructural de planta) quienes se encargan de controlar para cada puesto, el nivel de ruido, la luminosidad, la temperatura, la postura frente a la PC mediante el suministro de sillas y demás elementos de comodidad necesarios. También proveen los elementos de seguridad industrial como zapatos adecuados y vestimenta con los mínimos requisitos de seguridad.

- **Personal (de dirección, de operación, de desarrollo, otro)**

Las siguientes personas son quienes manejan – en diferentes niveles – información crítica o sensible para la organización. Por tal motivo ellos mismos son activos a considerar a la hora de evaluar la seguridad informática.

Gerente de Investigación y Desarrollo.
Gerente de Compras.
Gerente de R.R.H.H.
Gerente de Producción.
Gerente Administrativo.
Jefe de Planeamiento.
Responsable sistemas.
Jefe de M.A.H.P.I.
Jefe del depósito de Insumos.
Jefe del Pañol.
Jefe de mantenimiento (Ingeniería y talleres).
Jefe de los laboratorios físico – químico y microbiológico.
Jefe del Centro de Distribución (depósito de Producto Terminado).

- **Otros tangibles (edificaciones, mobiliario, instalación física)**

Sobre estos activos (que no serán detallados minuciosamente), sólo se hace mención a que todo lo referente a la seguridad de instalaciones, mobiliarios y edificaciones está controlado por MAHPI mediante los procedimientos constantemente monitorizados y evaluados por el Sistema de Gestión Integral (SGI, que ya fue mencionado en el relevamiento estructural de la planta).

El centro de cómputos está ensamblado sobre un piso técnico en el que se disponen el mobiliario del personal; el rack y mesas donde se apoyan los diferentes servidores y equipos de comunicaciones; las UPSs; el tablero de energía; la caja fuerte; los matafuegos; los

armarios de almacenamiento de carpetas y diferentes elementos de soporte o uso diario del departamento; las unidades de cintas de backup; la consola de los servidores.

2. Activos relacionados con el nivel de los Sistemas de Información.

- **Hardware (de proceso, de almacenamiento, de interfaz, servidores, firmware, otros)**

Se cuenta con 8 servidores y 136 estaciones de trabajo.
De éstas últimas 5 están destinadas a la automatización de la producción de planta e interactúan con los PLC mediante uno de los servidores.
De los restantes equipos 12 son móviles y los 119 son de escritorio.
Además hay 17 dispositivos de impresión (entre impresoras de alto rendimiento de red y de etiquetas de impresión remota). Dos de estas impresoras de red están abocadas a la facturación. Las tres impresoras de transferencia térmica permiten con sus etiquetas controlar la tras habilidad de los lotes de producción y la ubicación en los depósitos.
Hay también un equipo que brinda el servicio de conectividad a los equipos de radio frecuencia del centro de distribución.
Por más detalles ver relevamiento estructural; el resumen se aprecia en el siguiente cuadro:

Puestos	131
SCADAs	5
Servidores	8
Imps. de red	13
Imps. de etiquetas	3
Plotters de red	1
Puntos de acceso de Radio Frecuencia	3
Panel de Operaciones. PLC	2
	166

- **Software (de base, paquetes, producción de aplicaciones, modificación de firmware)**

Listado de software cuyo uso – por sectores – ya fue mencionado al final del relevamiento estructural de la planta:
Software de base y software de aplicación:

- Sistemas Operativos: de la plataforma Microsoft tanto para el equipamiento informático como para el de automatización SCADA; Unix (en el Data Center de Arcor, plataforma Sun); OS/400 para la plataforma AS/400 de IBM con la que se gestiona la mayor parte de los módulos comerciales y varios de los administrativos.
- Bases de datos: Informix para los sistemas de control de calidad y mantenimiento mecánico; para los equipos centralizados la base de datos es administrada mediante Oracle. Se está implementando una nueva solución para todos los sistemas centralizados de gestión (para toma de decisiones).
  Se posee un equipo que mediante una antena satelital es servidor de cotizaciones de bolsa contratado mediante la agencia CMA (de origen brasilero).
- Software Ofimático: soporte de Microsoft; Antivirus de McAfee; Correo y aplicaciones asociadas mediante Lotus Donimo.
- Comunicaciones: Se garantizan mediante la gestión de conexiones redundantes al data center. Existe una alta disponibilidad de los datos y la operatividad de los sistemas centralizados gestionando rutas redundantes entre los diferentes sitios de Arcor con el Data Center.
- Aplicaciones publicadas: Se realizan mediante conexiones por *Terminal Server*; *Citrix*; clientes de *emulación de AS/400*; aplicaciones replicadas mediante *Lotus Domino*; y mediante web servers y aplicaciones web como *Intranet*.
  No hay ninguna aplicación publicada que se gestione desde este sitio de Arcor.

Firmware:
PLCs, están bajo el control, mantenimiento y actualización del personal de ingeniería de planta.

- **Comunicaciones (redes propias, servicios, componentes de conexión, etc.)**

La siguiente descripción se puede apreciar en el esquema de la red informática presentado en el relevamiento estructural de sistemas.
El corazón de la red es el switch central (solución de chasis) que, mediante placas de puertos UTP y Fibra óptica (FO), enlaza todo el equipamiento informático del sitio y los equipos de comunicaciones.

Mediante la placa de fibra brinda conectividad a 6 switch periféricos. Con esto se destaca que toda la red está switcheada.
Mediante las placas de UTP garantiza la conectividad a equipos del sector Norte, los servidores y los routers de comunicaciones.
Los routers balancean la carga de requerimientos de comunicación en tres líneas (de dos proveedores diferentes), dos de las cuales son de fibra óptica y la restante de par de cobre.
Todo el cableado UTP es de categoría 5+ y las líneas internas de FO son multimodo con un par de líneas de backup cada una. La línea de FO hacia el sector de portería es subterránea y está especialmente diseñada para ello.
Las líneas de FO y par de cobre de comunicaciones hacia el exterior, como así los routers son de propiedad y administración de los proveedores correspondientes. Esto está regido por sendos contratos establecidos desde el área de Tecnología Informática de Arcor. Es oportuno mencionar que los routers comunican a los diferentes sitios de Arcor y hacia el Data Center mediante la red pública encriptando los paquetes de información. Ningún personal de Arcor posee gestión sobre éstos equipos, pero sí se posee un perfil para ver las configuraciones y el comportamiento de los diferentes routers. Los proveedores brindan un servicio vía web en el cual el soporte informático de cada base de Arcor y los responsables de TI pueden monitorear en modo gráfico la performance de los routers y los enlaces de comunicaciones.

3. Activos relacionados con el nivel de la Información.

- **Datos (informatizados, concurrentes al o resultantes del Sistema de Información)**

Información almacenada en la base de datos Informix:

sistema de Control de Calidad;

mantenimiento mecánico y electrónico;

sistema de control y seguimiento de tarjetas de mantenimiento, mejoras o reparaciones del SGI;

Datos generados por el servidor Lotus Domino:

correos de usuarios;

aplicaciones bajo dicha plataforma:

Sistemas de altas de productos;
Documentación y procedimientos de calidad;
Documentación y procedimientos de sistemas y tecnología informática;
Documentación a distribuir de Administración y de Investigación y Desarrollo;
Sistema de generación y control de prototipos;
Sistema de Remitos de materiales auxiliares;

Documentos de ofimática de usuarios y grupos de usuarios almacenados en servidores de archivos (fundamentales para el sistema SGI, entro otras);
Documentos de ofimática en equipos móviles o de usuarios;
Toda información almacenada en los mainframes ubicados en el data center o en la DMZ.

- **Meta-información (estructuración, formatos, códigos, claves de cifrado)**

Configuración de servidores; base de datos; servicios de correo; determinados servicios brindados por los servidores; logon scripts de usuarios; configuraciones de impresoras de red y/o térmicas; configuraciones de actualización de antivirus; configuraciones de pantallas de radiofrecuencia; configuraciones y administración de switch; configuraciones y administración todo lo referente al ingreso de personal a planta.
Configuración de los clientes Metaframe; Citrix; Browsers para intra o Internet.
Claves de acceso como administrador a Servidores y/o estaciones de trabajo y claves de caja fuerte.
Archivos ejecutables de los diferentes sistemas y sus archivos de configuración e instructivos de instalación.
Software instaladores de sistemas diversos, sistemas operativos; de recuperación de impresoras y demás periféricos.

- **Soportes (tratables informáticamente, no tratables)**

Discos instaladores de impresoras; servidores y sistemas diversos.
Cintas de backups diarias, mensuales e históricas.
Cintas o CD de backup varios.
Manuales e instructivos en CD, papeles y carpetas.
Listados e informes generados habitualmente mediante las impresoras.

4. Activos relacionados con el nivel de las Funcionalidades de la organización.

- **Objetivos y misión de la organización**

Arcor es una empresa industrial y comercial. La seguridad deberá garantizar estos macro objetivos.

Toda acción de seguridad deberá ser aplicada correctamente para no entorpecer el logro de este fin.

Por ende todos los recursos anteriormente relevados/mencionados se emplean para la realización de la misión de la empresa y deberán ser tomados en cuenta dependiendo de su nivel de criticidad.

- **Bienes y servicios producidos**

Toda la gama de productos de chocolate y alfajores fabricados en el sitio y todos los servicios de logística del centro de distribución.

- **Personal usuario y/o destinatario de los bienes o servicios producidos**

Todos los empleados están afectados en una u otra medida - todos están involucrados en el SGI.

Los primeros y principales destinatarios de los bienes y servicios producidos son los transportistas y las distribuidoras que trabajan con Arcor.

Al final de la cadena se encuentra el consumidor final que puede ser alguien en casi cualquier parte del planeta dado el nivel de las exportaciones de la empresa.

5. Otros Activos no relacionados con los niveles anteriores.

- **Credibilidad (ética, jurídica, etc.) o buena imagen de una persona jurídica o física.**

También es de incumbencia de la seguridad informática la protección de la reputación de la empresa. Algún incidente de seguridad puede quitar credibilidad, falta de confianza o directamente pérdida de negocios. Por ejemplo se puede perder una exportación: si una auditoría de una firma comercial del exterior fuera afectada, o una auditoría de los sistemas de Calidad ISO 9001 o HACCP no fuera satisfactoria: Análisis de Peligros en Puntos Críticos de Control; entre otros.

- **Conocimiento acumulado,**

El conocimiento que posee el soporte informático, pero sobre todo el personal de Investigación y Desarrollo; ingenieros de producción y mantenimiento y el de las demás áreas involucradas.
Es de gran importancia que haya procedimientos comunes y excepcionales para cubrir posibles ausencias. También deberían estar documentados.

- **Intimidad de una persona física,**

Privacidad de los datos personales. No sólo la información disponible en recursos humanos sino también por ejemplo el correo electrónico; los datos de carpetas personales; etc. En definitiva todo lo que se refiera a la protección de datos personales. En Argentina existe la Ley 25326 - Protección de los Datos Personales.

- **Integridad material de las personas, etc.**

Involucra todo lo referido a la seguridad física de las personas.
A los fines de este trabajo se puede considerar que toda acción realizada por el área de MAHPI colabora para alcanzar el nivel de seguridad necesario que se pretende en este punto.

Interpretación y análisis de la información recolectada.

Consolidación de identificación de activos para la seguridad informática: tomando los activos vistos desde MAGERIT, la evaluación del personal de tecnología y el resultado de las encuestas a usuarios clave. (Ver Anexo 3 – Encuesta a usuarios - Consolidación)

Se identificaron los activos de la información con el riego que poseen (medido) y se consignaron en la planilla siguiente. Se repite que la información fue tomada mediante encuestas basadas en el modelo OCTAVE y el análisis se basó en las guías MAGERIT.

En la siguiente planilla se puede apreciar cada activo con el valor de importancia dado por los usuarios clave.
Se han consignado las vulnerabilidades y amenazas de cada activo y se calcula el riego mediante la siguiente fórmula:

*Riesgo calculado = importancia * (vulnerabilidad + amenaza)*

Nota: importancia: valoración del activo desde el punto de vista del soporte informático y de los usuarios clave;
vulnerabilidad + amenaza: es el valor estimado con el cual el activo en cuestión es afectado.

En otra columna he consignado los controles de seguridad que ya están aplicados. Estos controles disminuyen el riesgo según la siguiente fórmula:

*Riesgo efectivo = importancia * (vulnerabilidad + amenaza - atenuación)*

Nota: atenuación: disminución del impacto por controles aplicados.

Sobre los activos con mayor *riesgo efectivo* hay que aplicar controles de seguridad. He seleccionado aquellos con un puntaje mayor a 12. El objetivo del trabajo es aplicar controles basados en la norma IRAM-ISO 17799, sobre Seguridad Informática, para disminuir dicho riesgo al menos a 12 puntos.

ACTIVOS	Importancia	VULNERABILIDADES	AMENAZAS	grado de impacto de Amen. y Vuln.	RIESGO Calculado	Con
Organizacionales						
Personas (confidencialidad)	5.000	estancamiento, falta de capacitación	Traspaso entre sectores, manejos incorrectos de la info	3.5	**17.5**	Es y r pra
Información en equipos móviles	5.000	fragilidad y versatilidad del equipo	virus, accesos externos, robos	4	**20**	Ba
Software de cotizaciones	5.000	Desperfecto o desgaste del servidor	Perdida de sincronismo de la antena satelital	4	**20**	Re se se y c pro so Ac pro co
Información en equipos de usuarios	4.625	no hay backup	virus, accesos externos	3.5	**16.188**	Co arc crí se
Sistemas de Investigación y desarrollo	5.000	confidencialidad	spyware	4	**20**	Es ba ac co
Sistemas administrativos	5.000	integridad y disponibilidad	corte de comunicaciones	5	**25**	Se Da Re co

ACTIVOS	Importancia	VULNERABILIDADES	AMENAZAS	grado de impacto de Amen. y Vuln.	RIESGO Calculado	Con
Correo electrónico	4.625	cuotas, indisponibilidad confidencialidad	, correos no deseados	5	**23.13**	Es ba ac co
Sistemas de RRHH	5.000	integridad, disponibilidad		4	**20**	Re tel
Sistemas de pedidos y facturación	5.000	integridad, disponibilidad		5	**25**	Re tel
Información crítica en Servidores	4.846	falta de capacidad en disco, integridad y confidencialidad	divulgación, filtraciones, hacking y spyware	4	**19.385**	Es ba fal es alg An co Fa co se co
Sistemas de gestión industrial, costos, balance de masa, etc.	4.833	lentitud	disponibilidad	3	**14.5**	Re tel
Sistema de control de calidad	5.000	disponibilidad, integridad y confidencialidad				Es ba Fa co se co

ACTIVOS	Importancia	VULNERABILIDADES	AMENAZAS	grado de impacto de Amen. y Vuln.	RIESGO Calculado	Con
Manuales, Procedimientos, Instructivos del Sistema de Gestión Integral	5.000	deterioro, extravío		2	**10**	La do res
Sistema de legislación	4.000	ubicado en PC local - no se hace backup		2	**8**	Se ins ac
Información variada en Servidores	3.000	integridad y disponibilidad		1	**3**	Es ba ac co
Información histórica de clientes (carpetas físicas)	5.000	deterioro, extravío				Ar tor es
Información histórica de proveedores (en papeles)	5.000	deterioro, extravío				Ar tor es
Información de haccp y pcc	5.000	integridad y disponibilidad	Problemas con el servidor			Ar tor es
Información en papel generada cotidianamente en impresoras	4.000	extravío		2	**8**	Sir im

ACTIVOS	Importancia	VULNERABILIDADES	AMENAZAS	grado de impacto de Amen. y Vuln.	RIESGO Calculado	Con
Infraestructura						
Switch central	5.000	fallas de fuentes, placas, conectores		5	**25**	Do rec de div UF elé bu co ac Inv sw pu
Switch periféricos	5.000	desperfectos del equipo o partes	acceso físico de personal no autorizado	3	**15**	Sw ac los pe es Mu rel pr ac Inv sw pu

ACTIVOS	Importancia	VULNERABILIDADES	AMENAZAS	grado de impacto de Amen. y Vuln.	RIESGO Calculado	Con
Router y equipos de comunicaciones	5.000	Desperfectos de equipos	accesos no autorizados	5	**25**	Co co tel de na int rec co rou Dia an
Servidor de base de datos (Calidad)	5.000	fallas varias del servidor o configuración	virus, intrusos y otras amenazas lógicas	5	**25**	Pla es se ex rep im es de (ve Se Se

ACTIVOS	Importancia	VULNERABILIDADES	AMENAZAS	grado de impacto de Amen. y Vuln.	RIESGO Calculado	Con
Servidor y estaciones de trabajo SCADA	5.000	fallas varias del servidor o configuración	virus, intrusos y otras amenazas lógicas	5	**25**	Ge Ing co em co co co Se un pro se
Servidor de Correo local	5.000	fallas varias del servidor o configuración	virus, intrusos y otras amenazas lógicas	4	**20**	Pla es se ex rep Se un pro se pro Se Se
Servidor de programación de producción	5.000	fallas varias del servidor o configuración	virus, intrusos y otras amenazas lógicas	5	**25**	Pla es se ex rep

ACTIVOS	Importancia	VULNERABILIDADES	AMENAZAS	grado de impacto de Amen. y Vuln.	RIESGO Calculado	Con
Servidores de archivos	5.000	capacidad de almacenamiento limitada, fallas del equipo	virus, intrusos y otras amenazas lógicas	4	**20**	Pla es se ex rep Se un pro se pro Se Se
Cableados de fibra óptica internos	5.000		cortes accidentales	4	**20**	To fib un
Cableados de fibra óptica externos al sitio	5.000		cortes accidentales o cortes del servicio programados	5	**25**	Co de tel de na int rec co Dia an
Cableados UTP	4.000		cortes	2	**8**	Inv sw pu

ACTIVOS	Importancia	VULNERABILIDADES	AMENAZAS	grado de impacto de Amen. y Vuln.	RIESGO Calculado	Con
Equipos móviles de gerentes	4.000	fragilidad y versatilidad del equipo	virus, accesos externos, robos	3	**12**	Eq co ma téc
Equipos de usuarios	4.333	obsolescencia, información cada vez más abundante	factibles de ser robados o que se les quite un componente	3	**13**	Ex ba ma téc co
Impresoras de red para facturación	5.000	Roturas por desgastes	indisponibilidad de insumos, mal uso	4	**20**	Es se ter se rec de
Impresora de RRHH	4.000	disponibilidad, confidencialidad		4	**16**	Co téc má de ce
Impresoras térmicas de etiquetas	4.000	fallas por funcionamiento continuo		4	**16**	Co téc me
Impresora de oficina de SGI	3.000	disponibilidad	usos inadecuados,	3	**9**	Co téc
Impresoras de usuarios	4.000	roturas	indisponibilidad de insumos	3	**12**	Ex im en

ACTIVOS	Importancia	VULNERABILIDADES	AMENAZAS	grado de impacto de Amen. y Vuln.	RIESGO Calculado	Con
Consola de monitorización de servidores	2.000	desperfectos del equipo		2	**4**	
UPSs	3.000	fallas de las baterías	apagado accidental, alta tensión	5	**15**	Es ca ca im ex ele qu he inc me
Racks de equipos	3.000		golpes y malos tratos	1	**3**	
Equipos de radiofrecuencia	4.000	malos tratos, caídas	corte de comunicaciones	4	**16**	Se la tec eq ga en es téc
Access Point de Radio Frecuencia	4.000	Access Point inalámbricos sin seguridad aplicada	Accesos no autorizados mediante conexiones inalámbricas a la red corporativa	4.5	**18**	Se inf tec eq ga en

ACTIVOS	Importancia	VULNERABILIDADES	AMENAZAS	grado de impacto de Amen. y Vuln.	RIESGO Calculado	Con
Unidad de Backup	5.000	desperfectos del equipo, atascos de cintas		4	**20**	Eq
Cintas de backups	5.000	deterioro, atascos	mal uso, robos	4	**20**	alr fue
Caja fuerte	5.000		incendio, violación	4	**20**	Es ac co
Clave de apertura de caja fuerte	5.000		olvido o pérdida	2	**10**	Do so
Sistema de Prototipos y seguimiento de proyectos	5.000	disponibilidad, integridad, confidencialidad	accesos no autorizados	5	**25**	Ba Se se se
Claves de acceso como administrador a Servidores	5.000		olvido o pérdida	5	**25**	Do y e Pe Bs ad los
Claves de acceso como administrador a Estaciones de trabajo	5.000		olvido o pérdida	4	**20**	Do y e Pe Bs ad los

ACTIVOS	Importancia	VULNERABILIDADES	AMENAZAS	grado de impacto de Amen. y Vuln.	RIESGO Calculado	Con
Archivos ejecutables de los sistemas	5.000	disponibilidad		4	**20**	Ba Fa se se co
Archivos de instructivos de instalación de sistemas	3.000		borrado accidental	2	**6**	Ba
Archivos instaladores de sistemas y sistemas operativos	3.000		borrado accidental	2	**6**	Ba
Configuración de Servidores	5.000	disponibilidad	eliminación accidental	3	**15**	Do so
Configuración de Bases de Datos	5.000	disponibilidad	eliminación accidental	3	**15**	Do so ba
Configuración de las impresoras de red	3.000	disponibilidad		4	**12**	Do so
Configuración de actualización del antivirus	3.000	disponibilidad		2	**6**	Do so
Configuración y administración de Switchs	3.000	disponibilidad		2	**6**	Do so
Documentación de respaldo del SGI	5.000	disponibilidad, confidencialidad, integridad		4	**20**	Ba Fa co se co
Configuraciones de clientes de Citrix	3.000	disponibilidad		1	**3**	Do so

ACTIVOS	Importancia	VULNERABILIDADES	AMENAZAS	grado de impacto de Amen. y Vuln.	RIESGO Calculado	Con
Configuraciones de clientes de Metaframe	3.000	disponibilidad		1	**3**	Do so
Archivos de configuración de sistemas	4.000	disponibilidad		2	**8**	Ba
Manuales e instructivos en papel o CD	4.000	disponibilidad	deterioro, destrucción,	1	**4**	gu de
Sistema de remitos materiales auxiliares	3.000	disponibilidad		3	**9**	Ba Fa co se co
Impresoras de facturación	5.000	disponibilidad, desgaste, roturas		5	**25**	Re im co téc co eq (cl rep im en có

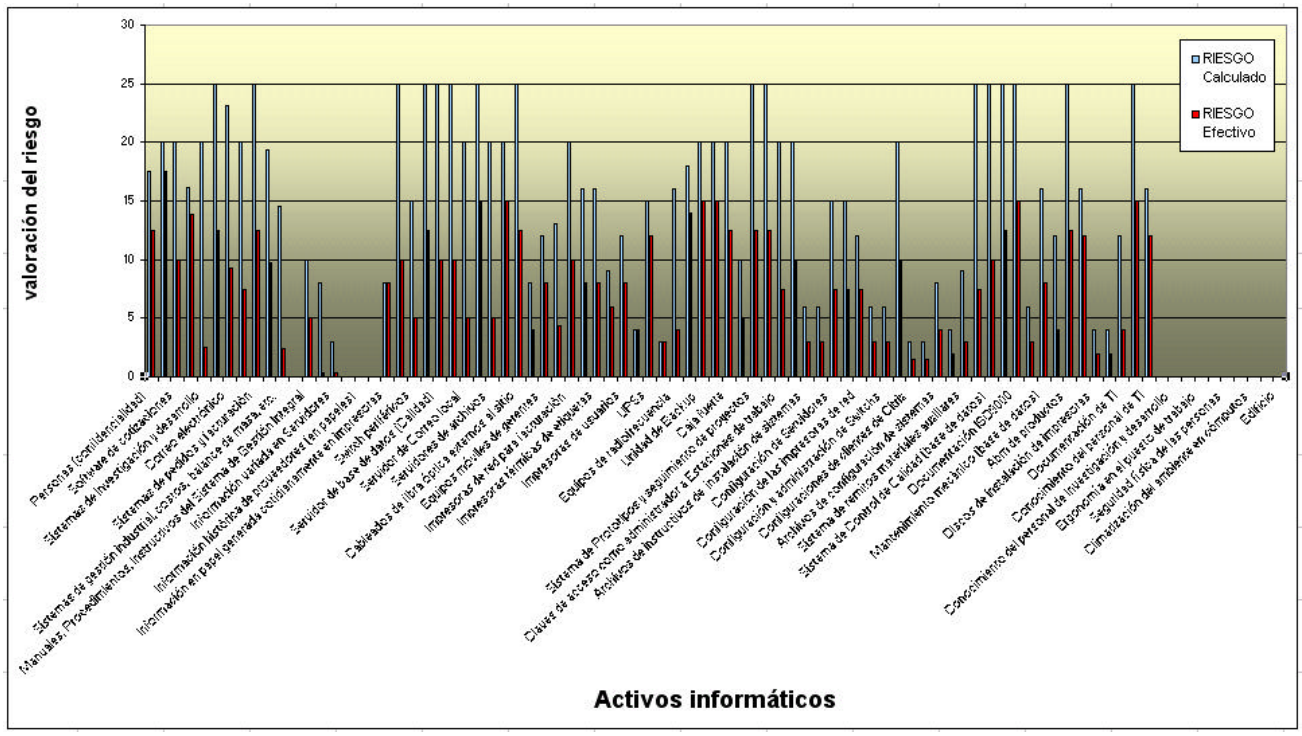
ACTIVOS	Importancia	VULNERABILIDADES	AMENAZAS	grado de impacto de Amen. y Vuln.	RIESGO Calculado	Con
Sistema de Control de Calidad (base de datos)	5.000	disponibilidad, confidencialidad		5	**25**	Ge so de co Fa co se co
Información almacenada o procesada en el data center	5.000	disponibilidad, integridad, disponibilidad		5	**25**	Ge GS cu inf so fur niv
Documentación ISO9000	5.000	disponibilidad		5	**25**	Ba Fa co se co
Logon script de usuarios	3.000	integridad, disponibilidad		2	**6**	Ba
Mantenimiento mecánico (base de datos)	4.000	disponibilidad		4	**16**	Ge so de co
Tarjetas de SGI (base de datos)	4.000	disponibilidad		3	**12**	Ge so de co

ACTIVOS	Importancia	VULNERABILIDADES	AMENAZAS	grado de impacto de Amen. y Vuln.	RIESGO Calculado	Con
ABM de productos	5.000	disponibilidad, confidencialidad		5	**25**	Ge so de res el
Documentación Administrativa	4.000	disponibilidad		4	**16**	Ba
Discos de instalación de impresoras	2.000	disponibilidad		2	**4**	gu de
Discos de instalación de servidores	2.000	disponibilidad		2	**4**	gu de
Documentación de TI	4.000	disponibilidad, confidencialidad		3	**12**	Re rer
PLCs	5.000	Desperfectos de equipos	Falta de comunicación entre los diferentes equipos, manipulación incorrecta, cortes de energía imprevistos	5	**25**	Ge Ing co em un co Es co nu eq
Conocimiento del personal de TI	4.000	renuncia, confidencialidad, indocumentación		4	**16**	Do
Conocimiento de Gerentes y Jefes de área	5.000	desactualización				En

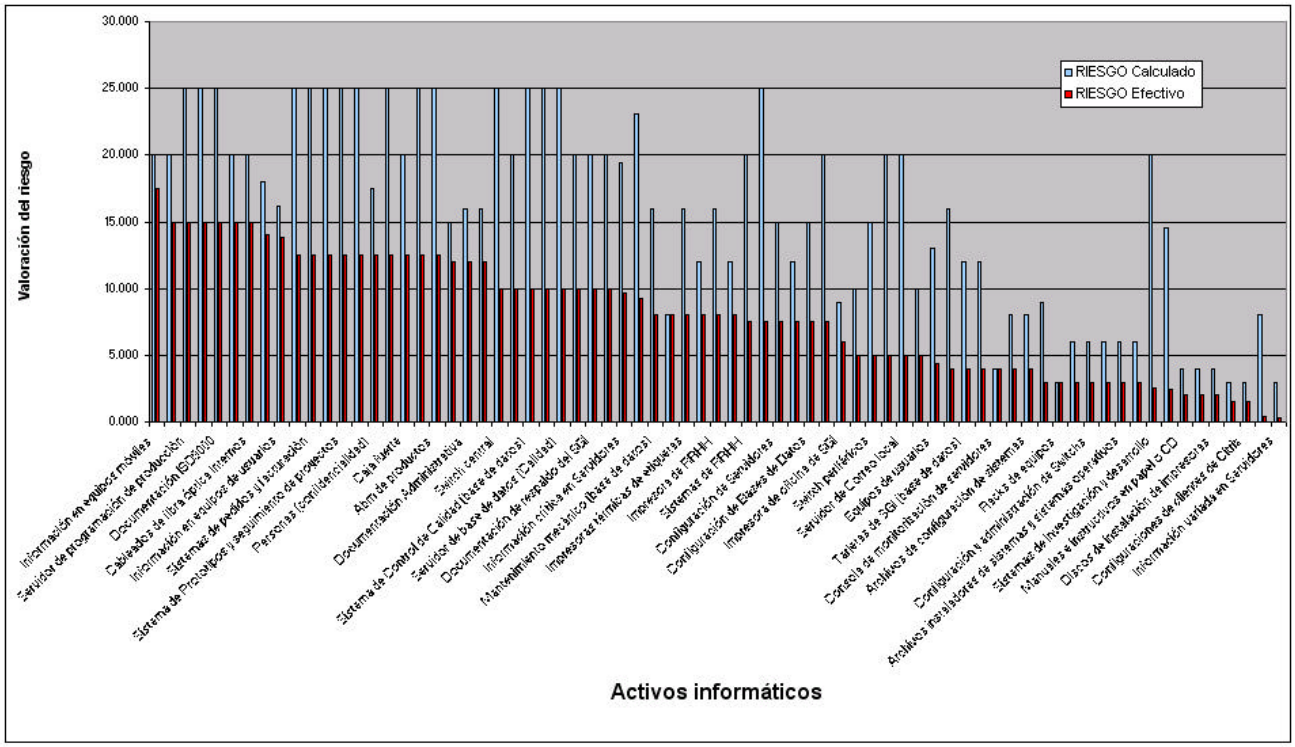
ACTIVOS	Importancia	VULNERABILIDADES	AMENAZAS	grado de impacto de Amen. y Vuln.	RIESGO Calculado	Con
Conocimiento del personal de investigacióny desarrollo	5.000					En
Conocimiento de ingenieros de producción y mantenimiento	5.000					En
Ergonomía en el puesto de trabajo	2.000					Co MA
Vestimenta de seguridad industrial	2.000					Co MA
Seguridad física de las personas	4.000					Co MA
Alarmas contra incendio y matafuegos	4.000	roturas, descargas, suciedad				Co MA
Climatización del ambiente en cómputos	3.000		falta del servicio			Co Se
Muebles y útiles	2.000	deterioro	usos inadecuados, traslados			Co MA
Edificio	3.000					Co MA

Resumen gráfico de la valoración de riesgos de activos.

A continuación se puede apreciar gráficamente la importancia dada por los usuarios clave a cada activo (serie azul).
La serie roja representa el resultado de la operación del riesgo calculado con la valoración de la disminución del riesgo por controles ya aplicados (o sea el riesgo efectivo):



En el siguiente gráfico se presenta la misma información pero ordenada por el riesgo efectivo. Esta es la base a la hora de elegir el plan de continuidad de protección de activos. Se basa en el riesgo efectivo donde se consideran las necesidades más urgentes y críticas en relación con la continuidad de las operaciones.



Conclusión sobre el análisis de riesgos de activos identificados:

En definitiva se pueden observar los siguientes aspectos como prioritarios a la hora de encarar una acción preventiva:

Almacenamiento de información en equipos móviles;

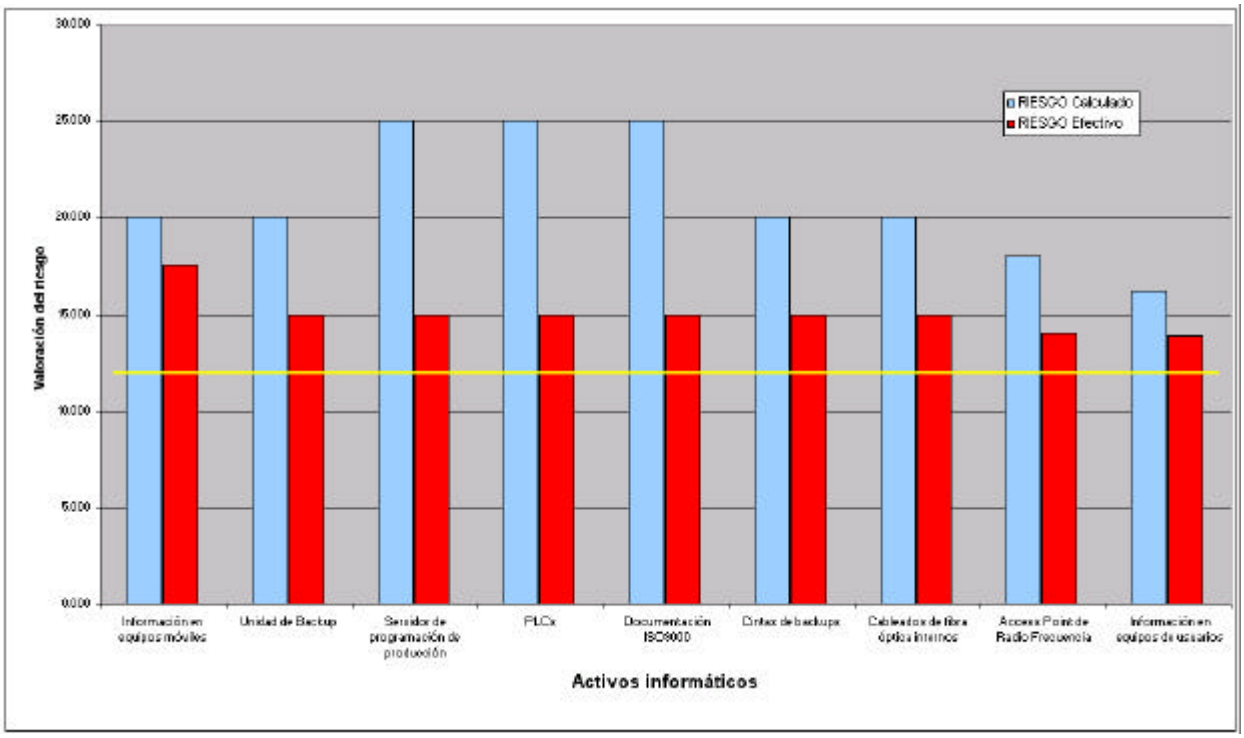
Asegurar equipos (móviles o de escritorios) sobre aspectos de seguridad lógica;

Información almacenada en servidores y sus servicios;

El resguardo de dicha información de forma segura y recuperable (Backups);

Capacitación – Concientización de las personas (conclusiones sobre las encuestas).

La línea amarilla grafica el objetivo del trabajo: reducir el riesgo efectivo de los activos informáticos por debajo de 12 puntos.



Conclusión sobre encuestas - preguntas abiertas:

De las preguntas que hacen referencia a la importancia de los activos se ve que están en concordancia con la identificación de los activos importantes. O sea que se reafirma la importancia de los activos ya identificados.

A la pregunta: *¿Qué aspectos de esta encuesta consideraría discutir con más detalle?* algunos han expresado que desean revisar el tema de "Políticas de seguridad y procedimientos al respecto"; también se refieren a que no saben acerca de lo relacionado con Seguridad Informática y cómo hacer más segura la información.

En cuanto a *¿Qué asuntos importantes no están cubiertos por esta encuesta?* figuraron la falta de capacitación relacionada con Seguridad Informática y lo referente a la comunicación de políticas o estrategias de seguridad informática. También requieren que haya capacitación al respecto. En un caso se notó la preocupación sobre cuáles son los procedimientos para el intercambio de PC's de una persona a otra, dado que se necesita estar seguro que la información y determinadas configuraciones no se propaguen sin control.

Al consultar sobre el *conocimiento de políticas de seguridad, procedimientos o prácticas* se ha mencionado que existen prácticas de backup pero se desconocen los detalles. También se ha recogido que se conoce que existen perfiles de usuarios para trabajar con todos los sistemas y que éstos están más o menos controlados (tampoco conocen detalles al respecto).

Para la pregunta *¿La estrategia de protección de la compañía es efectiva?* se vuelve a destacar en general la falta de conocimiento.

Conclusión sobre encuestas - preguntas cerradas:

Conocimiento de la seguridad y entrenamiento:
Mayoritariamente las personas dicen entender la problemática de la seguridad y su responsabilidad, pero advierten que no han recibido capacitación alguna al respecto.

Estrategia de la Seguridad:
En cuanto a la estrategia de seguridad de la compañía la mayoría afirma no conocer sobre tema. Si bien, algunos afirman que se aplican consideraciones de seguridad a las estrategias del negocio, la mayoría luego afirma o que no hay documentación, o no se actualizan o simplemente no se comunican; o directamente no saben del tema.

Administración de la Seguridad:
Para la administración de la seguridad he recogido casi la totalidad de respuestas "No sabe". Las preguntas abarcaban temas como la asignación de fondos para la seguridad; si la empresa a la hora de vincular o desvincular personas toma consideraciones de seguridad; si se hacen evaluaciones de riesgos y se toman acciones para mitigarlos.

Políticas y Regulaciones de Seguridad:
Al igual que el tópico anterior las respuestas fueron de total desconocimiento sobre tema.
No se sabe si hay políticas; por ende tampoco se está en condiciones de decir si se revisan, actualizan y comunican periódicamente. Tampoco se está en condiciones de afirmar si se poseen procedimientos más o menos establecidos para estas actividades de actualización y menos para saber sobre los esfuerzos que se hacen por estar actualizados.

Administración en colaboración sobre la seguridad:
A la pregunta "*¿Tiene la organización políticas y procedimientos para proteger la información cuando se trabaja con otras organizaciones?"* la mitad de las personas han contestado que sí. Pero cuando se le pidió una aclaración indicaron claramente una confusión con los procedimientos de seguridad de acceso al establecimiento fabril que sigue el departamento de RRHH. Si bien estos procedimientos aportan un aspecto importante para la seguridad de la información, no era éste el punto que se buscaba consultar. Por lo tanto éste aspecto es un complemento del anterior que hace referencia a las políticas. Conclusión: si las hay se desconocen totalmente.

Planes de Contingencia:

Para este aspecto resalta también un desconocimiento de las prácticas que pueda tener la compañía.

Planes y Procedimientos para la Seguridad Física:

En este punto ya hay más conocimiento porque las personas por lo general están al tanto de las prácticas que llevan en conjunto las áreas de RRHH y MAHPI al respecto. Si bien no abarcan todos los aspectos de la seguridad física (desde el punto de vista de la información) son procedimientos que se comunican y realizan.

Control del Accesos Físico:

Aquí hubo una clara confusión con el punto anterior. Se debe destacar que, si bien la mayoría de las respuestas fueron positivas, no existen políticas ni procedimientos de acceso. Hay sí restricciones mediante puertas con cerraduras al centro de cómputos y a ciertas oficinas.

Administración de Sistemas y Redes:

Al respecto se contestó mayoritariamente que sí hay planes para salvaguardar los sistemas; que hay procedimientos claros de backups y que el personal técnico conoce sus responsabilidades al respecto y actúa en consecuencia.

Autenticación y Autorización:

Se afirma que hay políticas y procedimientos documentados para otorgar y quitar derechos de acceso a la información pero debo destacar que la falta aquí está nuevamente en la comunicación.

Administración de Incidentes:

Se recogió una respuesta casi en su totalidad de ignorancia al respecto de procedimientos para detectar, reportar y actuar bajo incidentes sospechosos de seguridad.

Prácticas del Personal en General:

En relación a si *las personas tienen buenas prácticas de seguridad* muchos contestaron que sí. Dada la importancia de esta pregunta se les volvió a consultar y todos respondieron que "sí" en relación a sí mismos (cabe recordar que se trata de usuarios clave por sector) pero que "no", o "no saben" cuando se refieren a las demás personas.

Propuesta

A partir de los resultados de las encuestas y del trabajo de investigación propio he llegado a las siguientes conclusiones sobre las cuales basé la continuación del trabajo y mis propuestas:

Bajo el criterio de mayor criticidad, urgencia y la continuidad de las operaciones del negocio he resaltado los aspectos con mayor prioridad de tratamiento (siempre tomando el punto de vista del usuario de los sistemas informáticos de Arcor):

Capacitación – concientización de las personas en cuanto a la seguridad informática. Haciendo hincapié en la confidencialidad de la información manejada.

Cuidado de la información almacenada en servidores y los servicios prestados por éstos.

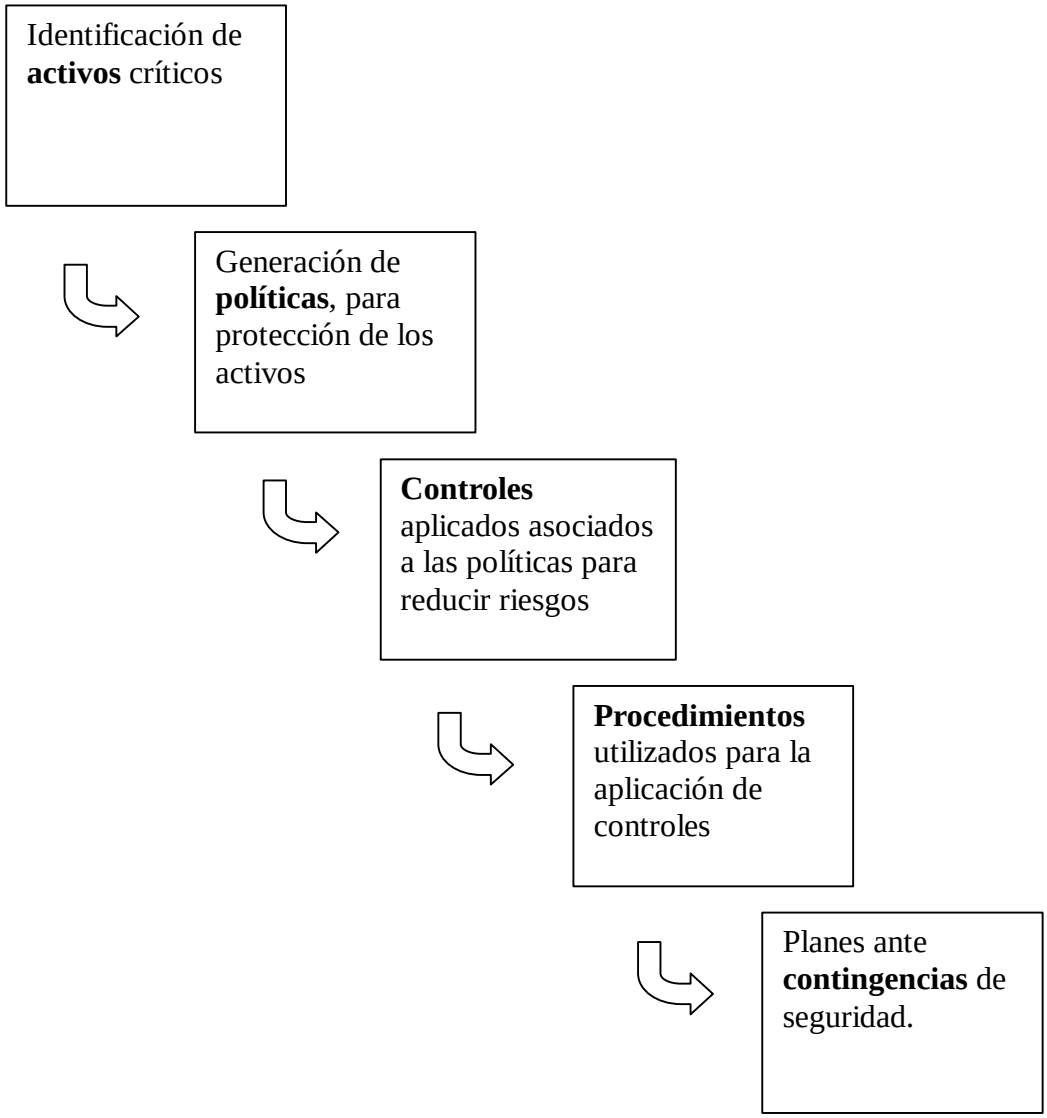
Atención y cuidado del almacenamiento de información en equipos móviles (utilizados por usuarios de mayor cuidado en lo referente a la confidencialidad). Se incluye concientización de riesgos; backup de la información.

Buscar asegurar los equipos (móviles o de escritorios) contra accesos no permitidos haciendo hincapié especialmente en los aspectos de seguridad lógica.

Concretamente, y siguiendo la metodología indicada al comienzo del trabajo, se proponen políticas particulares para cada aspecto identificado.
Luego siguiendo la norma ISO 17799 se aplican los controles asociados a las políticas para reducir el riesgo de los activos.
Seguidamente se detallan algunos procedimientos – guías, para efectivizar la aplicación de los controles
Por último se indican, a modo de ejemplo, algunos planes de contingencia ante eventos de seguridad informática.
(ver esquema en la página siguiente)

Esquema de la metodología seguida.

El siguiente esquema ilustra aquello que he implementado a raíz del análisis previo donde se identificaron los activos informáticos más críticos. El criterio de selección ha sido tomar los activos con puntaje de riesgo efectivo mayor a 12 puntos. El objetivo es lograr reducir estos valores al menos a 12 puntos.



Activos seleccionados.

Resumen de activos identificados de mayor riesgo con un resumen de tareas a implementar y su referencia a la norma IRAM-ISO 17799

ACTIVOS	Acciones a implementar	Referencia al control de la norma IRAM-ISO 17799
Información en equipos móviles	Backup periódico y documentado; capacitación e implementación de cifrado de carpetas. Aplicar políticas NTFS y seguridad en el registro.	7.2.5 Seguridad del equipamiento fuera del ámbito de la organización 8.4.1 Resguardo de la información 9.8.1 Computación móvil 8.3.1 Controles contra software malicioso 10.3.2 Cifrado 9.5 Control de acceso al sistema operativo
Unidad de Backup	Incorporarlo a los equipos críticos inventariados por el soporte técnico externo	5.1.1 Inventario de activos 8.4.1 Resguardo de la información
Servidor de programación de producción	Implementar todas las políticas de seguridad del registro de Windows y de los volúmenes NTFS tal cual lo tienen implementados los demás servidores.	8.3.1 Controles contra software malicioso
PLCs	implementación de UPS (Ya ha sido comprada e instalada por Ingeniería– Mantenimiento eléctrico.)	7.2.2 Suministros de energía
Documentación ISO9000	Modificar la metodología del backup (debe ser full diario) y hacer una reingeniería de cómo y dónde se están almacenando los diferentes documentos. Se implementará la nueva versión del software de backup (sin costo por haberse comprado en su momento una versión protegida por dos años).	8.4.1 Resguardo de la información 8.6.3 Procedimientos de manejo de la información
Cintas de backups	Hacer copias al menos de las cintas históricas y guardarlas en otra ubicación física.	8.4.1 Resguardo de la información 8.6.1 Administración de medios informáticos removibles
Cableados de fibra óptica internos	Se hará un inventario riguroso de switch, funciones y puestos de trabajo	8.5.1 Controles de redes 7.2.3 Seguridad del cableado 5.1.1 Inventario de activos
Access Point de Radio Frecuencia	Implementar una configuración de seguridad robusta en los Access Point	8.5.1 Controles de redes 9.4.7 Control de conexión a la red
Información en equipos de usuarios	Aplicar políticas NTFS y seguridad en el registro. Concientizar sobre la importancia de almacenar información importante en los recursos de los servidores	8.3.1 Controles contra software malicioso 9.5 Control de acceso al sistema operativo 8.6.3 Procedimientos de manejo de la información 8.7.5 Seguridad de los sistemas electrónicos de oficina

Propuesta de políticas de Seguridad Informática.

Habiendo identificado los activos con nivel de riesgo más apremiante, se proponen para asegurar los mismos y como medida para concientizar a las personas, las siguientes políticas de seguridad informática. Se tomaron como referencia los lineamientos de políticas de "The SANS™ Institute" (The Trusted Source for Computer Security Training, Certification and Research: http://www.sans.org - junio de 2005)[16]

Antes de incorporarlas al trabajo han sido consensuadas con el gerente Operativo, el gerente de Control de Calidad de planta y el gerente de Coordinación de Calidad Corporativa.
Como políticas sugeridas que son, se reconsiderarán cuando las gerencias de Seguridad Informática y Recursos Humanos corporativas acuerden políticas definitivas para todo el grupo.
A partir de este trabajo se elevó por parte de las gerencias que se consultaron (mencionadas en el párrafo anterior) una solicitud de incorporación de un nuevo párrafo en la Política General del Sistema de Gestión Integral (ver Anexo 1).

El coordinador de calidad destacó lo siguiente a raíz de las consultas:

> "...son políticas bien formuladas: lo suficientemente amplias y no muy restrictivas como para ser aceptadas ..."

Referenciando la evaluación final de una auditoría de calidad realizada a una planta industrial de ARCOR (que no es la de estudio en el presente trabajo) destacó el siguiente párrafo:

> " Aspectos débiles resultantes del cumplimiento de los requisitos a cumplimentar para lograr el Premio Iberoamericano de Excelencia en la Gestión:
>
> ✍✍...
> ✍✍Asegurar y mejorar la validez, integridad y seguridad de la información."

Con esto destacaba que el tema de la generación de la información, la gestión y el cuidado de la misma ya están incorporándose diferentes procedimientos de auditoría de sistemas de calidad. Acentuó lo pertinente del trabajo y sugirió que la temática debe ser considerada en un párrafo aparte dentro de la Política General del Sistema de Gestión Integral. Afirmaba que desde dicho

[16] The SANS Security Policy Project ; The SANS Institute; 8120 Woodmont Avenue, Suite 205 Bethesda, Maryland 20814, http://www.sans.org/resources/policies - marzo de 2005

sistema se genera conocimiento e información que son vitales y que hay que velar por su seguridad.

Seguidamente solicitó que se redacte dicho párrafo para elevarlo por los canales pertinentes a fin de incorporarlo en la política mencionada.

Para ello agregó las siguientes consideraciones para tener en cuenta:

> "Palabras para incluir en la política:
> Asegurar y mejorar la validez, integridad y seguridad de la información.
> Accesibilidad, integridad, relevancia, oportunidad, utilización y distribución de la información."

Fundamentó sus sugerencias con el siguiente párrafo extraído del manual de auditoría para el Premio Iberoamericano de Excelencia en la Gestión donde se hace referencia a la importancia de la gestión de la información:

> Analiza cómo la organización gestiona sus recursos internos, por ejemplo: los financieros, de información, de conocimientos, tecnológicos, de propiedad intelectual, materiales y recursos externos, incluidas las asociaciones con proveedores, distribuidores, alianzas y órganos reguladores, con el fin de apoyar la eficiente y eficaz gestión de la misma.

A partir de estas sugerencias le he propuesto el siguiente párrafo:

> Asegurar la información generada y gestionada por el sistema cuidando los aspectos de integridad, disponibilidad y confidencialidad.

Pero, luego de otra entrevista concluimos que, el párrafo a sugerir para su inclusión en la Política General del Sistema de Gestión Integral sea:

> ***Asegurar la disponibilidad, integridad y confidencialidad de la información.***

Cabe aclarar que cada párrafo de la Política General del Sistema de Gestión Integral está respaldado por una serie de documentos y procedimientos específicos más extensos.
El párrafo propuesto se respaldará con las políticas que se generen desde las gerencias de Seguridad Informática y Recursos Humanos corporativos, como ya se mencionó.
A la espera de éstas, se proponen políticas específicas para fundamentar las acciones, tareas y procedimientos implementados en el presente trabajo para reducir el riesgo de los activos identificados con mayor criticidad.

Política de Seguridad informática - ARCOR SAIC – Div. Chocolates.

La Política de Seguridad Informática de la División Chocolates de Arcor tiene como escenario la Política General del Sistema de Gestión Integral del Grupo. (Anexo 1 – "Política del Sistema de Gestión Integral – S.G.I.")

Para ello busca fundamentarse en los principios que guían este sistema aportando los aspectos de Seguridad Informática necesarios.

Es objetivo de la misma aportar un apoyo considerable para mantener *"el liderazgo en el Mercado Interno a través de un fuerte desarrollo de nuevas tecnologías, equipamientos..." ...*

" Para lograr estos objetivos, industrialmente, surge que debemos focalizarnos en acelerar los procesos de mejora continua para:

Aumentar la flexibilidad de las líneas de producción, los índices de calidad, disminuir drásticamente las pérdidas y desvíos de consumo, devoluciones de clientes e indisponibilidad de equipos, asociados a un incremento en los niveles de limpieza, seguridad y cuidado del medio ambiente de las plantas." (Anexo 1, segunda página – "Implementación del SGI en la Planta de Colonia Caroya")

Para lograr esta alineación a las políticas generales de Arcor, la Seguridad Informática se fundamenta en la norma IRAM-ISO IEC 17799:

> "La información y los procesos, sistemas y redes que le brindan apoyo constituyen importantes recursos de la empresa. La confidencialidad, integridad y disponibilidad de la información pueden ser esenciales para mantener la ventaja competitiva, el flujo de fondos, la rentabilidad, el cumplimiento de las leyes y la imagen comercial." (de norma IRAM-ISO IEC 17799, Pág.9)

La presente política deberá enmarcarse dentro de la Política General de Seguridad Informática del Grupo ARCOR, llegado el momento, podrá modificarse parcial o totalmente.

La Gerencia de Seguridad Informática junto con la Gerencia de Tecnología de la Información serán quines establezcan y acuerden con el Directorio y las diferentes Divisiones de la Compañía dicha Política General.

Justificación:

Los activos involucrados en la generación, modificación, almacenamiento y resguardo de la información son recursos de importancia y vitales para la Compañía. Por tal motivo y para evitar pérdidas operativas, productivas, financieras o confidenciales la gerencias Operativa, de Calidad, de Recursos Humanos, de Desarrollo y Administrativa de la Planta de ARCOR SAIC -

División Chocolates de Colonia Caroya debe estar comprometida en la preservación, utilización y mejora de dichos activos.

Responsabilidades:

Dirigencia:

Es responsable de dar a conocer y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad acordadas en la presente política. Están incluidos todos los gerentes y jefes de área.

Soporte Informático:

Es responsable de establecer los controles de seguridad apropiados para cada usuario o grupos de usuarios y supervisar el uso de los recursos informáticos, de llevar a cabo las tareas de seguridad relativas a los sistemas sobre los cuales brinda soporte, como por ejemplo, aplicar los parches correctivos cuando le llegue la notificación del fabricante o de la Gerencia de Seguridad o Tecnología Informática.

Es responsable de informar a la dirigencia y a sus superiores sobre toda actividad sospechosa, evento amenazador o intrusión.

También se prevé que el soporte informático sea responsable de coordinar el análisis de riesgos con cierta periodicidad, planes de contingencia y prevención de desastres. Así también será el responsable de coordinar eventos de concientización y capacitación sobre Seguridad Informática. Para todo ello cuenta con el apoyo de la red de soportes técnicos y funcionales que Arcor dispone.

Usuarios:

Son responsables de cumplir con todos los enunciados relativos a la seguridad informática mencionados en estas políticas y en particular de:

- ?? Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos.
- ?? No divulgar información confidencial de la Compañía a personas no autorizadas.
- ?? No permitir o facilitar el uso de los sistemas informáticos de la Compañía a personas no autorizadas.

?? No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax) para otras actividades que no estén directamente relacionadas con el trabajo en la Compañía.

?? Proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida.

?? Reportar inmediatamente a su jefe inmediato cualquier evento que pueda comprometer la seguridad de la Compañía y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades sospechosas.

Política de Uso aceptable de equipos informáticos.

1.0 Apreciación Global

La intención de la Gerencia de Seguridad Informática no es imponer restricciones contrarias a la cultura de confianza, franqueza e integridad de ARCOR. La Gerencia de Seguridad Informática se compromete a proteger a los empleados de ARCOR y a la compañía de las acciones perjudiciales o ilegales cometidas por individuos, ya sea con conocimiento de causa o no.
Se deja mención que todos los sistemas utilizados mediante Internet o intranet; los equipos de computación, el software; sistemas operativos; los medios de comunicación y almacenamiento, las cuentas de correo electrónico; por ejemplo, son propiedad de ARCOR. Así mismo también cabe aclarar que estos sistemas serán usados para los propósitos del negocio sirviendo los intereses de la compañía.

La seguridad eficaz es un esfuerzo de equipo que involucra la participación y apoyo de cada empleado de ARCOR que trata con información y/o sistemas de información. Por lo tanto, es responsabilidad de cada usuario conocer las siguientes pautas y actuar de acuerdo a ellas.

2.0 Propósito

El propósito de esta política es generar un perfil de uso aceptable de equipos de computación en ARCOR. La intencionalidad es proteger tanto al empleado como a la compañía. El uso impropio de dicho equipamiento expondrá a ARCOR a riesgos como ser ataques de virus; comprometer los sistemas o la red; dificultar los diferentes servicios prestados; o derivar en problemas legales.

3.0 Alcance

Esta política se aplica a los empleados, contratistas y consultores que trabajan en ARCOR. Así mismo, se aplica a todo el equipamiento informático que posee, es alquilado o se usa en ARCOR.

4.0 Política

4.1 Uso general y propiedad

1. Los administradores de la red desean proveer un razonable nivel de privacidad, sin embargo los usuarios deben ser concientes que los datos que generen en los sistemas corporativos serán propiedad de ARCOR. Debido a la necesidad de proteger la red, la dirigencia no garantiza la confidencialidad de la información almacenada en cualquier dispositivo de red.
2. Los empleados son responsables de aplicar buen criterio y racionalidad en sus actividades. Cuando algo no esté expresamente mencionado en esta política los empleados deben consultar a sus supervisores o gerentes.
3. Se recomienda que cualquier información que los usuarios consideren sensible o vulnerable esté cifrada.
4. Por propósitos de seguridad o mantenimiento de la red, el personal de mantenimiento de la red está autorizado a monitorear el equipamiento, los sistemas y el tráfico de la red en cualquier momento.
5. ARCOR se reserva el derecho a auditar la red y los sistemas periódicamente para asegurar el cumplimiento con esta política.

4.2 Seguridad y Propiedad de la Información

1. La información debe estar clasificada como confidencial o no confidencial. Las diferentes gerencias deben hacer esta clasificación y el soporte de tecnología debe suministrar los medios para su almacenamiento seguro. Los usuarios de información confidencial (por ejemplo: datos privados de la compañía; estrategias corporativas; secretos de marketing; especificaciones; lista de clientes; información de investigación…) deben realizar todo lo necesario para prevenir accesos no autorizados a dicha información.
2. No se deben compartir las cuentas de usuarios y las contraseñas se debe guardar en lugar seguro. Los usuarios son responsables de la seguridad de sus cuentas y contraseñas. Las contraseñas se deben cambiar cada dos meses.
3. Todas las PCs y notebooks deben estar protegidas por un protector de pantalla que se active automáticamente como máximo a los 10 minutos de no utilizarse.
4. La información crítica debe estar cifrada. (Ver política de cifrado más adelante.)
5. Dado que las notebooks son especialmente vulnerables se debe tener un especial cuidado.

6. Todo equipo conectado a la red de ARCOR debe tener instalado y actualizado el antivirus corporativo definido por el equipo de Tecnología Informática de ARCOR.
7. Los empleados deben tener especial cuidado al abrir correos electrónicos con anexos de origen desconocido dado que pueden contener virus o códigos maliciosos.

4.3. Usos inaceptables

Las siguientes actividades, en general, están prohibidas.

Bajo ninguna circunstancia un empleado de ARCOR está autorizado a cometer alguna actividad ilegal mientras utilice recursos propios de ARCOR.

La siguiente lista intenta proveer un marco de actividades catalogadas como de uso inaceptable. No se pretende que sea exhaustiva.

Sistema y actividades de red

Las siguientes actividades están estrictamente prohibidas, sin excepciones:

1. Violaciones de los derechos de cualquier persona o compañía protegidos por “copyright”, patentes u otra propiedad intelectual incluyendo la instalación o distribución de software “pirata” u otro del cual ARCOR no tenga la correspondiente licencia de uso.
2. Copiar material licenciado sin autorización, por ejemplo: digitalización o distribución de fotografías de revistas, libros, música de los cuales ARCOR o el usuario final no tenga la respectiva licencia.
3. Exportar software, información técnica, software de encriptación o tecnología, en violación de leyes de control de exportación internacionales o regionales
4. Introducción de programas maliciosos en la red o servidores (por ejemplo: virus, gusanos caballos de Troya)
5. Revelar su password o permitir el uso de su cuenta de usuario a otros.
6. Usar los activos informáticos de ARCOR para transmitir material o realizar actividades que comentan violaciones de acoso sexual o de violencia.
7. Hacer ofertas fraudulentas de productos o servicios originados por o desde ARCOR.
8. Realizar *cortes* o interrupciones en la red.
   Los cortes incluyen, entre otras actividades, el acceso a datos de los cuales no se es el destinatario; “loguearse” en un servidor; utilizar una cuenta de usuario a la que no se esté

expresamente autorizado; etc.

Las *interrupciones* incluyen acciones como network sniffing, pinged floods, packet spoofing, denial of service, y cualquier ruteo de información con propósitos maliciosos.

9. El scaneo de puertos está expresamente prohibido a menos que medie una notificación anterior de la Gerencia de Seguridad Informática.
10. Ejecutar cualquier forma de monitorear la red interceptando información al menos que sea parte de las tareas habituales del puesto de trabajo.
11. Conseguir mediante engaño cualquier autenticación de usuario o información de seguridad de algún equipo, servidor, red o cuenta de usuario.
12. Utilizar cualquier programa, script o comando; o enviar cualquier clase de mensajes con la intención de interferir, deshabilitar o finalizar sesiones de usuario.
13. Proveer información de listas de empleados o sobre ARCOR a terceras partes fuera de la compañía.

Actividades de correo electrónico y comunicaciones

1. Enviar mensajes de correo electrónico no solicitados. (correo electrónico spam).
2. Cualquier forma de daños vía correo electrónico o teléfono, ya sea por el lenguaje utilizado, la frecuencia o el tamaño de los mensajes.
3. Usos no autorizados o modificaciones de los encabezados de correos electrónicos.
4. Crear o remitir cualquier tipo de cadenas de correos.
5. Uso de correos no solicitados originados dentro de ARCOR y que ofrecen servicios de la compañía.
6. Envío de correo electrónico o similar que no esté relacionado con las actividades del negocio.

5.0 Incumplimientos

Cualquier empleado que se encuentre en violación de esta política podrá tener una sanción disciplinaria acorde con las políticas y procedimientos de la gestión de RRHH de ARCOR.

Política de contraseñas

1.0 Introducción

Las contraseñas son un aspecto importante de la seguridad informática. Es una primera protección para la utilización de cuentas de usuario. La elección de una contraseña pobre podría comprometer la red corporativa de Arcor. Todos los empleados (incluyendo terceras partes que accedan a los sistemas de la compañía) deben seguir los pasos apropiados, para seleccionar y asegurar sus contraseñas.

2.0 Propósito

El propósito de esta política es establecer un estándar para la creación, protección de contraseñas fuertes y la frecuencia de cambio de las mismas.

3.0 Alcance

El alcance incluye a todo el personal que tiene o es responsable de una cuenta de usuario (o cualquier forma de acceso que soporte o requiera una contraseña) en cualquier sistema de Arcor; o que tenga acceso a la red o a cualquier información de Arcor que no sea pública.

4.0 Política

4.1 General

- ?? Todas las contraseñas de sistema (por ej.: de administrador de servidores o dominios, cuentas de administración de aplicaciones, etc.) deben ser cambiadas al menos cada dos meses.
- ?? Las contraseñas de usuarios deben ser administradas de forma centralizada por Seguridad Informática.
- ?? Todas las contraseñas de nivel de usuarios (por ej.: correo electrónico, accesos a Internet, computadores, etc.) deben cambiarse al menos una vez por trimestre.
- ?? Las contraseñas no deben ser insertadas en mensajes de correos ni en ninguna forma de comunicación electrónica.
- ?? Todas las contraseñas (ya se del nivel de sistema o de usuario) deben ajustarse a las siguientes indicaciones.

4.2 Guías generales

A. Guías generales de generación de Contraseñas

Las contraseñas de usuarios son usadas para varios propósitos. Algunos de los más importantes son: cuentas de usuarios, accesos a Internet, cuentas de correo electrónico, inicio de sesión en servidores o activos de red.

Todas las personas deben saber cómo seleccionar contraseñas robustas.

Contraseñas con las siguientes características se pueden clasificar como pobres o débiles:

- ?? Tiene menos de ocho caracteres
- ?? Es una palabra que se pueda encontrar en un diccionario (en idioma español u otro).
- ?? Es una palabra de uso común como ser:
    - o Nombres de familia, mascotas, amigos, colegas, etc.
    - o Términos y nombres de computación, comandos, sitios, compañías, hardware o software.
    - o Palabras como “ARCOR”, “sanjose”, “sanmartin” o cualquier derivación.
    - o Cumpleaños o cualquier información personal como dirección o número de documento o teléfono.
    - o Palabras o números que sigan un patrón como “aaabbb”, “qwerty”, “zyxwvuts”, “123321” “123456789”, etc.
    - o Cualquier ejemplo mencionado deletreado al revés.
    - o Cualquier ejemplo mencionado seguido o precedido por un número (por ej: admin1, 1admin).

Para contraseñas robustas se pueden enumerar las siguientes características:

- ?? Contienen tanto letras mayúsculas como minúsculas (por ej.: a-z, A-Z)
- ?? Tienen caracteres numéricos y de puntuación (por ej.: 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- ?? Al menos contiene ocho caracteres alfanuméricos.
- ?? No contiene ninguna palabra en algún lenguaje, jerga, dialecto, etc.
- ?? No está basada en información personal, nombres de familia, etc.
- ?? Se deben crear contraseñas fácilmente recordables, por ejemplo puede basarse en un título de una canción o en una afirmación o en una frase. Por ejemplo, la frase puede ser

“Esta es una buena forma de recordar”, y la contraseña podría ser “eE1bFdR” o “E<E1bfd_r” u otra variación.

Las contraseñas nunca deben ser escritas en lugares visibles.

Nota: No se debe usar ninguno de estos ejemplos como contraseña.

B. Estándares de protección de contraseñas

No se deben usar contraseñas de la compañía para accesos de otros servicios externos. Cuando sea posible no se debe usar la misma contraseña para acceder a diferentes utilidades.

No se deben compartir las contraseñas con nadie, incluyendo secretarias o asistentes administrativos. Todas las contraseñas deben ser tratadas como información sensitiva y confidencial

Lista de cuidados:

- ?? No revelar una contraseña por teléfono a nadie.
- ?? No escribir contraseña en correos electrónicos
- ?? No revelar contraseñas a ningún jefe
- ?? No decir una contraseña en frente de otros
- ?? No mencione el formato de una contraseña (ej.: “mi apellido”)
- ?? No revelar contraseñas en cuestionarios o formularios de seguridad
- ?? No compartir contraseñas con familiares
- ?? No revelar contraseñas a colegas en vacaciones

Si alguien consulta por una contraseña, se le debe mencionar esta política y dirigirlo al soporte informático del sitio.

No se deben escribir contraseñas y guardarlas en la oficina. No la almacene en archivos de la computadora u algún dispositivo sin encriptar.

Se deben cambiar las contraseñas al menos una vez cada tres meses salvo las contraseñas de nivel de sistema. Éstas últimas deben cambiarse a lo sumo bimestralmente.

Si se sospecha que una cuenta está comprometida o se ha revelado una contraseña, se debe cambiar la contraseña y reportar el incidente al soporte técnico.

C. Estándares para desarrollo de aplicaciones

Los desarrolladores de aplicaciones deben asegurar que sus programas contienen las siguientes precauciones de seguridad. Las aplicaciones:

- ?? deben soportar autenticación de usuarios individuales y no de grupos de usuarios.
- ?? no deben almacenar las contraseñas en texto plano o mediante formas que sean fácilmente reversibles.
- ?? deben proveer una jerarquía de administración por roles donde cada usuario pueda hacer funciones sin necesidad de conocer otra contraseña que no sea la propia.

5.0 Incumplimientos

Cualquier empleado que se encuentre en violación de esta política podrá tener una sanción disciplinaria acorde con las políticas y procedimientos de la gestión de RRHH de ARCOR.

Política de seguridad en Servidores

1.0 Propósito

El propósito de esta política es establecer estándares para la configuración de servidores internos propios de ARCOR. La efectiva implementación de esta política minimizará el acceso no autorizado a la información y tecnología propias de la compañía.

2.0 Alcance

Esta política se aplica a todos los servidores propios y/u operados por ARCOR – Colonia Caroya.

3.0 Política

3.1 Propiedad y Responsabilidades

Todos los servidores de Arcor deben estar bajo la supervisión y mantenimiento del soporte técnico local. Dicho soporte cuenta con el apoyo del la Gerencia de Tecnología Informática mediante a red de soportes técnico – funcionales de ARCOR.

Cada soporte local deberá establecer un proceso para la actualización y configuración de los servidores los cuales serán revisados y aprobados por la Gerencia de Tecnología Informática.

- Los servidores deben estar registrados en los sistemas de inventario de hardware corporativo; de listas de control de actualización de servidores y en el manual de procedimientos e instructivos que ARCOR dispone corporativamente. Al menos deberá contar con la siguiente información.
  - Contacto de supervisión y mantenimiento: el soporte técnico y su reemplazo.
  - El sistema operativo y su versión además de la configuración básica del hardware.
  - Las principales aplicaciones o servicios brindados.
- La información en los sistemas de administración corporativos debe mantenerse actualizada.
- Los cambios de configuración deben seguir los procedimientos de administración de cambios apropiados.

3.2 Guías generales de configuración

- ?? La configuración de los sistemas operativos debe estar en concordancia con las guías brindadas por Tecnología Informática y Seguridad Informática.
- ?? Se deben deshabilitar todas las aplicaciones y servicios que no se usen.
- ?? El acceso a los servicios debe ser registrado y/o protegido por algún método de control de acceso.
- ?? Deben ser instalados los parches de seguridad más recientes tan pronto como sea posible, con la única excepción que al hacerlo interfiera con las operaciones del negocio.
  Para evitar posibles errores, las gerencias de Tecnología y Seguridad Informática, deberán aplicar dichos parches sobre entornos de pruebas semejantes a los más críticos que estén en producción.
- ?? Las relaciones de confianza entre sistemas deben evitase ya que implican riesgos de seguridad. Sobre todo si hay otras formas de comunicación posible.
- ?? Siempre se deben usar principios estándar de seguridad.
- ?? No se deben utilizar cuentas de administrador cuando la tarea requerida se pueda hacer mediante otra cuenta sin tantos privilegios sobre el sistema.
- ?? Si se dispone de un canal de conexión seguro, los privilegios de acceso deben utilizarse sobre dicho canal (por ej.: conexiones de red encriptadas utilizando SSH o IPSec).
- ?? Los Servidores deben estar físicamente ubicados en un entorno de acceso controlado.

3.3 Monitoreo

- ?? Todos los eventos relacionados con la seguridad sobre sistemas críticos o sensibles deben registrarse y auditarse tal como sigue:
  - o Todos los registros de seguridad deben permanecer en el sistema por lo menos una semana.
  - o Las cintas de backup semanales (backup full), ya sea de registros o información sensible y crítica, deben mantenerse al menos por un mes.
  - o Las cintas de backup mensuales (backup full) deben mantenerse por un mínimo de dos años.

?? Todo evento relacionado con la seguridad debe ser reportado a los soportes de Tecnología Informática o de Seguridad Informática.
Algunos de los eventos pueden ser:
- o Ataques de búsqueda de puertos abiertos.
- o Evidencias de accesos no autorizados a las cuentas de usuario con privilegios.
- o Ocurrencias de anomalías no relacionadas con las aplicaciones específicas de algún servidor.

3.4 Complacencia

?? Se deben hacer auditorias regularmente por organizaciones autorizadas por ARCOR.

?? Las auditorias se deben administrar por algún grupo interno de Tecnología Informática o Seguridad Informática.

?? Se debe prevenir que las auditorias no causen inconvenientes operacionales.

4.0 Incumplimientos

Cualquier empleado que se encuentre en violación de esta política podrá tener una sanción disciplinaria acorde con las políticas y procedimientos de la gestión de RRHH de ARCOR.

Política de Anti-virus

1.0 Propósito

Establecer requerimientos que deben cumplir todas las computadoras conectadas a la red de Arcor con el objetivo de asegurar una efectiva prevención y detención de virus.

2.0 Alcance

Esta política se aplica a todos los equipos informáticos de la compañía. Incluye, por ejemplo, las PCs de escritorio, notebook, Servidores de aplicaciones y de archivos.

3.0 Política

Todas las PC de Arcor deben tener instalado el antivirus estándar propuesto por Tecnología Informática. Debe utilizarse algún método para que se actualice automáticamente.
Los equipos que se encuentren infectados deben desconectarse de la red hasta que puedan ser revisados y se verifique que estén libres de virus.
El soporte técnico local es el responsable de la actualización de los antivirus en los diferentes equipos informáticos y de su revisión periódica.
Se debe configurar el equipo informático y el software antivirus de modo que no pueda ser desinstalado o deshabilitado por el usuario.
Cualquier actividad que tenga la intención de crear o distribuir programas maliciosos en la red de la compañía está totalmente prohibida.

Refiérase a los Procedimientos recomendados para Anti-virus de Arcor para prevenir problemas con virus.

4.0 Incumplimientos

Cualquier empleado que se encuentre en violación de esta política podrá tener una sanción disciplinaria acorde con las políticas y procedimientos de la gestión de RRHH de ARCOR.

Política de uso del correo electrónico

1.0 Propósito

Prevenir que se trasmita una mala imagen de la compañía. Cuando un correo electrónico es enviado fuera del dominio de la compañía, las personas en general lo ven como un mensaje oficial de dicha compañía.

2.0 Alcance

Esta política abarca el uso adecuado de cualquier correo electrónico que se envía desde la compañía y se aplica a todos los empleados y demás personas que usen el sistema de correo corporativo de Arcor.

3.0 Política

3.1 Uso prohibido

El sistema de correo electrónico de Arcor no puede ser utilizado para la creación o distribución de cualquier mensaje disociador u ofensivo incluyendo comentarios ofensivos o discriminatorios sobre raza, género, orientación sexual, creencias o prácticas religiosas, invalides, nacionalismo, pornografía, etc.

Tampoco puede ser utilizado para el envío de material que viole las leyes de propiedad intelectual: distribución de música, videos, etc.

Quienes reciban mensajes con contenidos de éste tipo desde personas dentro de Arcor deberán reportarlo a su supervisor inmediato.

3.2 Uso personal

Utilizar el correo electrónico provisto por Arcor para uso personal es sólo aceptado con restricciones. No se deben enviar ni seguir cadenas de correos.

3.3 Monitoreo

Las cuentas particulares de correo electrónico pueden ser supervisadas por personal técnico cuando sea necesario. Para ello deberá mediar una autorización explícita de los superiores inmediatos del técnico y de la persona a monitorear.

4.0 Incumplimientos

Cualquier empleado que se encuentre en violación de esta política podrá tener una sanción disciplinaria acorde con las políticas y procedimientos de la gestión de RRHH de ARCOR.

Política de encriptación aceptable

1.0 Propósito

El propósito de esta política es proveer una guía que limite el uso de encriptación a aquellos algoritmos que ya hayan recibido una revisión pública sustancial y hayan sido probadas efectivamente.

2.0 Alcance

Esta política se aplica a todos los empleados de la compañía.

3.0 Política

Los algoritmos de encriptación estándares como DES, Blowfish, RSA, RC5, IDEA, etc. deben ser usados como base para las tecnologías de encriptación. Dichos algoritmos son utilizados en el cifrado por aplicaciones ampliamente aceptadas. Por ejemplo Network Associates con su producto Pretty Good Privacy (PGP) usa combinaciones de IDEA, RSA, etc.; y Secure Socket Layer (SSL) utiliza encriptación RSA.

Los sistemas de criptografía simétrica deben usar llaves de longitud de al menos 128 bits. Para los sistemas de criptografía asimétrica (mediante llaves públicas y privadas) se deben utilizar llaves de longitud tal que permitan que el cifrado sea lo suficientemente seguro, al menos de 1024 bits.

El uso de algoritmos de encriptación propietarios no se permite bajo ningún propósito.

4.0 Incumplimientos

Cualquier empleado que se encuentre en violación de esta política podrá tener una sanción disciplinaria acorde con las políticas y procedimientos de la gestión de RRHH de ARCOR.

Política de comunicaciones inalámbricas

1.0 Propósito

La presente política prohíbe el acceso a la red de ARCOR por medio de comunicaciones inalámbricas inseguras. Sólo se permite las conexiones de aquellos sistemas inalámbricos que cumplan con los criterios de esta política.

2.0 Alcance

Esta política cubre todos los dispositivos de comunicación de datos inalámbricos (por ejemplo: PCs, PDAs) que estén conectados a la red interna de Arcor. Se incluyen todos los dispositivos inalámbricos capaces de transmitir paquetes de datos.

3.0 Política

3.1 Registro de Access Points y equipos conectados

Todos los access points inalámbricos conectados a la red corporativa deben estar registrados y aprobados por Tecnología Informática (mediante el soporte técnico local del sitio). Dichos access points deben ser controlados periódicamente para revisar si no han sido accedidos por dispositivos no autorizados. Todas las interfaces de red inalámbricas usadas en notebook u otro dispositivo deben ser registradas por Tecnología Informática.

3.2 Tecnología aprobada

Todos los equipamientos que utilicen acceso inalámbrico deberán ser de marcas y provistos por proveedores aprobados por Tecnología Informática. Deberán soportar las configuraciones de seguridad enumeradas en la presente política.

3.3 Encriptación y Autenticación

A los efectos de cumplir con esta política, todas las implementaciones deben utilizar algún método de encriptación de al menos 56 bits. Además, se debe filtrar el acceso mediante las direcciones de hardware (MAC address). Éstas deben registrarse y poder rastrearse.
En la medida en que el equipamiento lo permita debe usarse alguna forma segura de autenticación de usuarios previa a la aceptación de la conexión.

3.4 Configuración del SSID (Service Set Identifier)

El nombre de la red inalámbrica (SSID) no debe contener ningún identificador de la organización, como ser el nombre de la compañía o la división; el nombre de algún empleado o la descripción de un producto.

4.0 Incumplimientos

Cualquier empleado que se encuentre en violación de esta política podrá tener una sanción disciplinaria acorde con las políticas y procedimientos de la gestión de RRHH de ARCOR.

Aplicación de controles acordes a la norma IRAM-ISO 17799

(Objetivo: reducir el riesgo efectivo de activos críticos)

Se han implementado los controles más apremiantes según el análisis realizado anteriormente. La mayoría responden a la lista de activos a asegurar, pero también se incluyeron controles que, si bien no son urgentes o de mayor criticidad, fueron pertinentes implementar ya sea por la operatoria del centro de cómputos; los objetivos del Sistema de Gestión Integral y/o el presupuesto disponible para el caso.

Para cada activo identificado como crítico se consigna la aplicación de controles con una tabla similar a la siguiente.

En ella se puede identificar el activo en estudio, la norma IRAM-ISO 17799 de referencia; la política asociada a cumplir; el valor del riesgo efectivo y el valor del riesgo que se pretende luego de la aplicación de los controles.

También se consigna el tiempo en que fue implementado el control (se enumeran por orden de implementación):

Activo identificado como crítico	Referencia a la Norma IRAM-ISO 17799	Política de seguridad asociada	Riesgo efectivo	Riesgo esperado
Descripción del activo	X.X.X Capítulo de referencia de la norma	Política que se pretende cumplir	XX puntos	XX puntos

Tiempo efectivo de aplicación: Momento en el cuál o desde el cuál se implementó el control.

1 - Controles aplicados sobre equipos de computación en general:

Activo identificado como crítico	Referencia a la Norma IRAM-ISO 17799	Política de seguridad asociada	Riesgo efectivo	Riesgo esperado
Información en equipos de usuarios	8.3.1 Controles contra software malicioso 9.5 Control de acceso al sistema operativo 8.6.3 Procedimientos de manejo de la información 8.7.5 Seguridad de los sistemas electrónicos de oficina	✍ Uso aceptable ✍ Contraseñas	13.8 puntos	10 puntos

Tiempo efectivo de aplicación: sobre todos los equipos de usuarios desde Octubre de 2004.

Mejoras obtenidas:

Disminución de incidentes por problemas de configuración de equipos y considerable reducción de instalación de software no licenciado.

Controles aplicados:

Los controles aplicados restringen el acceso remoto e instalaciones de software. Otros previenen contra tareas erróneas de los usuarios (intencionales o no).

En la aplicación de estos controles de seguridad he necesitados realizar varias pruebas. El objetivo de mejorar la seguridad de las estaciones de trabajo era logrado, pero algunas aplicaciones no funcionaban correctamente o directamente no iniciaban, como es el caso del cliente de correo corporativo, o los clientes del sistema de programación de la producción. Puede verse el detalle en el instructivo anexado más abajo en el apartado "Procedimientos" en la página 134.

Cabe aclarar que luego de haber llegado a esta conclusión se fueron incorporando nuevos equipos (mediante el plan y presupuesto de mantenimiento anual del equipamiento informático) y a todos se les aplicaron estas directivas.

La cantidad de equipos nuevos aproximadamente es de 20, pero a la vez muchos de los equipos anteriores se rotaron hacia otros usuarios y se les cambió el sistema operativo, permitiendo aplicar las políticas mencionadas.

También hay que considerar la siguiente diferenciación de equipos a los cuales se les aplicó alguna directiva de seguridad diferente.

Para la generalidad de equipos:

Como ya lo mencioné los usuarios inician sesión con privilegios de USUARIOS locales. Además mediante el editor de políticas de grupo se le restringe utilidades de configuración que pudieran perjudicar el buen funcionamiento del equipo. Por ejemplo no se permite el ingreso al "Panel de Control".
Se deshabilita la cuenta de administrador original del equipo.
Se genera una nueva cuenta de administrador local y se le asigna una contraseña (almacenada en un sobre en la caja fuerte existente en el Centro de Cómputos).
Se deshabilita la cuenta de invitado y cualquier cuenta administrativa que venga incorporada con el equipo.

Diferencia aplicada en equipos de uso múltiple en planta:

Además de las anteriores se aplicaron las siguientes directivas:
Se deshabilitaron o quitaron las unidades de almacenamiento extraíbles.
Dado que usan un usuario común, se habilitó la configuración para que ingresen sin necesidad de loguearse (agiliza el arranque del equipo y evita equívocos en la contraseña de acceso, muchas personas utilizan la misma cuenta). Son 7 equipos. Resta por implementar lo mismo en otros 4. Para esto hay que cambiarles el sistema operativo, lo que requerirá una ampliación o cambio de hardware previamente.

Equipos con Sistema Operativos Windows 95 o Windows 98:

Cuando es necesario se configuran las políticas de equipo y usuario, disponibles en un entorno de Windows NT, con el propósito de acotar las operaciones de los usuarios sobre el sistema operativo.
Se incorporaron en un plan de recambio para ir migrando paulatinamente a sistemas operativos más actuales. Mencionado en el punto anterior.

Equipos con aplicaciones concretas:

No se les aplica ninguna directiva lógica a los dos equipos que interactúan con equipamiento de control de la viscosidad del chocolate.

Tampoco se consideró al equipo que administra las ranuras y molinetes de acceso porque está en un lugar físico seguro y tiene como Sistema Operativo MS-DOS 6.22 y no comparte recursos. Sólo graba cada 10 minutos la información adquirida de las ranuras en un servidor.

Detalle final al momento de la presentación del presente trabajo:

Sistema Operativo	cantidad de instalaciones	cantidad implementadas	Porcentaje
DOS	2	n/a	n/a
Win 95	36	n/a	n/a
Win 98	23	n/a	n/a
Win NTWS	9	9	100 %
Win 2000	19	17	89 %
Win XP	58	51	88 %
Win NT Server	6	n/a	n/a
Win 2000 Server	1	1	100 %

2 - Controles sobre equipos móviles:

Activo identificado como crítico	Referencia a la Norma IRAM-ISO 17799	Política de seguridad asociada	Riesgo efectivo	Riesgo esperado
Información en equipos móviles	7.2.5 Seguridad del equipamiento fuera del ámbito de la organización 8.4.1 Resguardo de la información 9.8.1 Computación móvil 8.3.1 Controles contra software malicioso 10.3.2 Cifrado 9.5 Control de acœso al sistema operativo	Uso aceptable Contraseñas Encriptación	17 puntos	10 puntos

Tiempo efectivo de aplicación: sobre todos los equipos móviles a partir de Octubre de 2004.

Mejoras obtenidas:

Además de las mencionadas para la generalidad de los equipos, se creció en la toma de conciencia sobre las vulnerabilidades y amenazas que tienen las PC portátiles.
Se mejoró el resguardo de la información.

Controles aplicados:

Se aplican los controles y directivas igual que al resto de los equipos más las consideraciones siguientes:

Concientización sobre cuidados de traslado y utilización del equipo móvil.
Precaución ante posibles robos en lugares públicos (aeropuertos, traslados, etc.)

Para la realización de **backups** de datos críticos locales se implementó un componente asociado al sistema de Backup que permite hacer el respaldo de la información que se seleccione en forma desatendida (el usuario y el administrador de sistemas no tienen que recordar hacer el respaldo, se hace automáticamente luego de una primera configuración)
La información, que se respalda en un disco del servidor, se graba en cinta semanalmente.
El agente de backup para equipos portátiles se instaló con una versión - licencia de prueba en cinco notebooks mientras se negocia la compra de las licencias definitivas. Los costos – de aproximadamente U$s 50 por cliente – se justifican ampliamente dada la importancia de la

información respaldada y la seguridad que brinda el software, tanto al interesado como al soporte técnico informático.
En dicha negociación se ha resaltado desde Tecnología Informática que se debe recordar que la política es guardar toda información crítica en los servidores y que los soportes técnicos locales de cada base no se responsabilizan por la información almacenada localmente en equipos de escritorio o móviles.
Sin embargo se propone la implementación de dicho software de backup para usuarios muy puntuales en los que coinciden las siguientes variables:

Personas que viajan al exterior con mucha frecuencia;
Personas de nivel jerárquico gerencial;
Personas con responsabilidades corporativas.

Dentro de éste grupo se encuentran el gerente de Investigación y Desarrollo; el gerente de Coordinación Corporativa de Calidad; el gerente de Compras y el Gerente de Recursos Humanos.

Para determinados niveles gerenciales, se le otorgó una **cuenta local de administrador** para el caso de necesitar realizar tareas de mantenimiento, configuraciones en otros sitios y/o instalaciones. (Su cuenta para uso habitual es como todos: Usuario local)

Cifrado de archivos confidenciales: Luego de varias pruebas he llegado a la conclusión de no poder cifrar los archivos en los equipos ya que en el entorno de dominios en que nos manejamos no trabaja adecuadamente. Cuando se cambia la contraseña de la cuenta en el dominio se pierde el acceso a los archivos cifrados. Tampoco el administrador local del equipo puede accederlos.
Para resolver este inconveniente se puede esperar la migración que Tecnología Informática de Arcor tiene previsto realizar hacia un entorno donde sí sea compatible el cifrado de archivos y carpetas. La otra alternativa es comprar software de cifrado para entornos Windows.

3 - Controles aplicados sobre equipos de Radio Frecuencia:

Activo identificado como crítico	Referencia a la Norma IRAM-ISO 17799	Política de seguridad asociada	Riesgo efectivo	Riesgo esperado
Access Points de Radio Frecuencia	8.5.1 Controles de redes 9.4.7 Control de conexión a red 10.3.2 Cifrado	✍ Comunicaciones inalámbricas ✍ Encriptación	14 puntos	10 puntos

Tiempo efectivo de aplicación: sobre todos los equipos de radio frecuencia y los respectivos access points en abril de 2005.

Mejoras obtenidas:

Acceso a la red inalámbrica con muy buen nivel de seguridad. Se restringió la cantidad de potenciales conexiones de equipos, que podrían reducir la performance de los equipos que tienen que trabajar sí o sí con dicha tecnología.

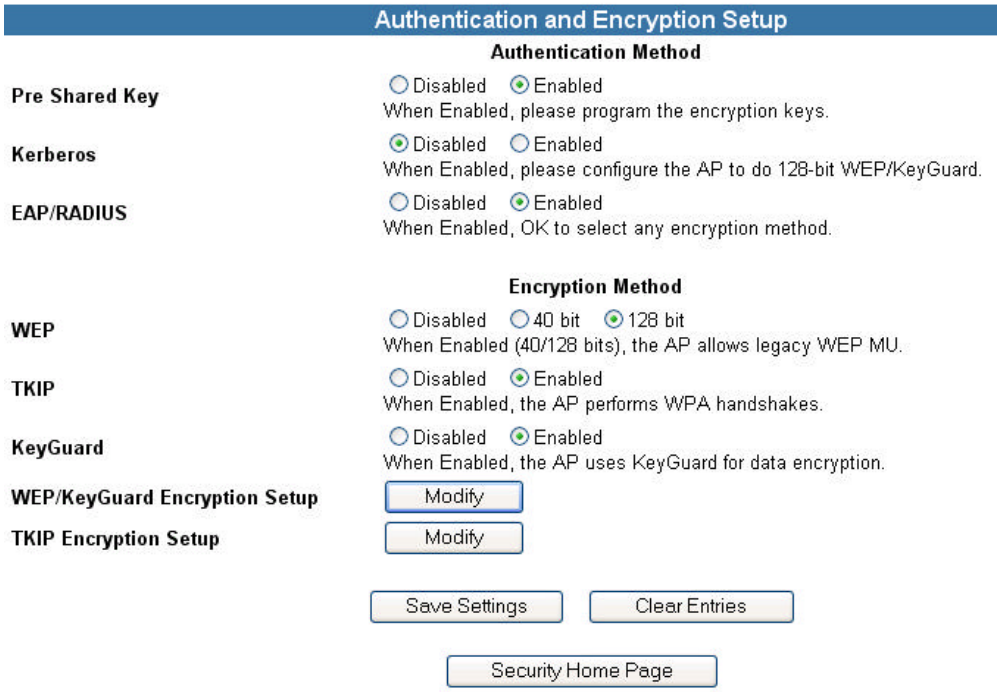
Controles aplicados:

Se aplicaron los siguientes controles:

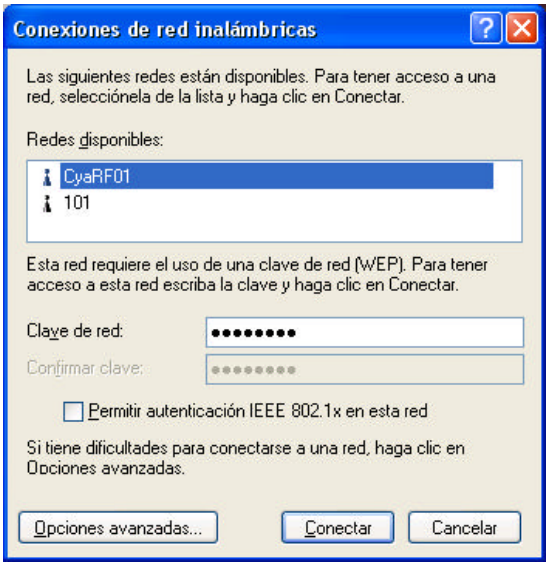
Se cambió la contraseña de administración remota que viene configurada por defecto en los Access Points.
Se cambió la identificación de la red inalámbrica que viene por defecto en los equipos.
Se implementó la comunicación con encriptación con clave de 128 bits.
Se enumeraron las direcciones físicas (MAC Address) de los equipos que deben tener acceso a la red inalámbrica y se registraron en la base de Procedimientos e Instructivos para su actualización. Ver la política para redes inalámbricas.
Se comprobó que todos los equipos de radiofrecuencia del centro de distribución trabajen correctamente con estos cambios.
La instalación final consta de 5 access points y 8 equipos móviles de trabajo. Se deja un access points en el primer piso para la utilización en las gerencias y salas de reuniones. Se habilitaron sólo cuatro notebooks para que puedan trabajar con la red inalámbrica, si fuera necesario.

Opciones más avanzadas de seguridad; como por ejemplo la autenticación de conexión por usuarios o que la descripción de la red no se publique abiertamente; no se pudieron implementar por no ser soportadas por las unidades móviles de trabajo.
El método de autenticación "kerberos" no se puede implementar porque no se tiene un esquema de Active Directory como lo ofrece un entorno de Windows 2003 server, por ejemplo.

La implementación en mayor detalle:
En la siguiente pantalla se presenta la pantalla de configuración de uno de los access points.



La siguiente pantalla ilustra la conectividad inalámbrica de una notebook en los momentos de prueba en plena implementación.
(Las diferentes identificaciones de redes fueron cambiadas en el momento de la implementación, las que se ven son las que vienen por defecto en los equipos o aquella descripción que se usó en las pruebas. Las direcciones física fueron deliberadamente modificadas.)



Identificación de la red inalámbrica

Se cambió de la estándar 101 por una personalizada (en el ejemplo CyaRF01)

Generación de una clave de encriptación simétrica:

La clave de encriptación se fijó en: ABCDEF01234567890123456789 (hexadecimal).

Se habilitó en los Access Points las siguientes direcciones físicas de equipos (MAC Address):

de Access Points

00:AA:FF:B1:38:DF	Centro de distribución Norte - Este
00:AA:FF:B2:3A:03	Centro de distribución Norte - Oeste
00:AA:FF:B3:39:53	Centro de distribución Sur - Este
00:AA:FF:55:DC:CD	Centro de distribución Sur - Centro
00:AA:FF:55:53:FD	Centro de distribución Sur - Oeste
00:AA:FF:55:13:C1	Oficinas Administrativas (backup para el Centro de Distribución)

de Equipos móviles del Centro de distribución:

00:AA:FF:EE:9E:66	Unidad Móvil 01
00:AA:FF:EE:A1:65	Unidad Móvil 02
00:AA:FF:EE:A1:64	Unidad Móvil 03
00:AA:FF:EE:A1:63	Unidad Móvil 04
00:AA:FF:EE:55:62	Unidad Móvil 05

de Equipos móviles del Centro de distribución (manuales)

00:AA:FF:DD:CC:D2	Unidad Móvil Manual 01
00:AA:FF:DD:CC:D1	Unidad Móvil Manual 02

de Notebooks con red inalámbrica ya configurada:

00:0D:31:F1:2E:66	Gerencia Operativa
00:0D:31:44:03:89	Gerencia de Investigación y Desarrollo
00:0D:31:44:49:AA	Jefe de Investigación y Desarrollo
00:0D:31:44:B9:99	Soporte Técnico Informático

de Notebooks a las cuales se prevee configurar:

00:0D:31:F1:3B:FF	Gerencia de Recursos Humanos
00:0D:31:F1:2E:65	Gerencia de Planta
00:0D:31:F1:2E:64	Gerencia Corporativa de Calidad

4 - Controles aplicados sobre el servidor de Programación de Producción:

Activo identificado como crítico	Referencia a la Norma IRAM-ISO 17799	Política de seguridad asociada	Riesgo efectivo	Riesgo esperado
Servidor de programación de producción	8.3.1 Controles contra software malicioso 8.4.1 Resguardo de la información 8.6.3 Procedimientos de manejo de la información	Uso aceptable Contraseñas Encriptación	15 puntos	12 puntos

Tiempo efectivo de aplicación: Abril de 2005.

Controles aplicados:

Si bien no hay un procedimiento ya estandarizado en Arcor para la configuración de seguridad de los servidores miembros Windows 2000, se tomó como base la guía para asegurar servidores con sistema operativo Windows NT Server. Esta guía, comparada y contrastada con la guía que Microsoft propone [17], sirvió como base para el procedimiento aplicado al servidor en estudio. Se puede consultar el procedimiento seguido en el apartado de "Procedimientos", más adelante.

Cabe aclarar que, en Arcor – Caroya, se está próximo a adquirir un nuevo servidor para un propósito específico y por lo tanto la guía seguida se aplicará también en dicho servidor.

[17] "Guía de operaciones de seguridad para Windows 2000 Server; Capítulo 4: Asegurar servidores basándose en su función"; www.microsoft.com/spain/technet/seguridad/2000server/chapters/ch04secops.aspx - abril de 2005.

5 - Controles aplicados sobre servidores de archivo:

Activo identificado como crítico	Referencia a la Norma IRAM-ISO 17799	Política de seguridad asociada	Riesgo efectivo	Riesgo esperado
Información en servidores de archivo	8.4.1 Resguardo de la información 8.6.3 Procedimientos de manejo de la información	Uso aceptable Servidores	15 puntos	12 puntos

Tiempo efectivo de aplicación: sobre todos los servidores de archivo en abril de 2005.

Mejoras obtenidas:

Se optimizó el espacio en disco. – En las encuestas fue recurrente la mención a inconvenientes por la falta de espacio de disco en los servidores.

Se agruparon los diferentes recursos según la afinidad de uso. – El uso desmedido y descomprometido del espacio por algunos sectores afectaba directamente a otros. Ahora cada sector administra los recursos que le han sido asignados.

Controles aplicados:

Se movieron los archivos y se modificó la forma de acceso a varios de los recursos.

Se cuidó especialmente que cada objeto (carpeta o documento) continúe con los permisos de usuarios y de grupos de usuarios que poseía con anterioridad.

La asignación de recursos a uno u otro servidor se analizó y consensuó con personal administrativo de planta, de control de producción, de sistemas y con los instructores de SGI.

Situación anterior: Los nombres de servidores y carpetas se han modificado por motivos de seguridad, los que se ven son simplemente orientativos para mostrar la tarea realizada.

Servidor 1

Información Control de Calidad y Oficina Técnica;

Servidor 2

Documentación de Administración; Registros de consumos de materias primas e insumos. Información inherente a capacitación, entrenamientos y Seguridad Industrial.

Servidor 3

Información técnica y planoteca de Ingeniería; información y registros de mantenimiento mecánico y eléctrico.
Archivos de uso del Sistema de Gestión Integral.
Información confidencial del sector de Investigación y Desarrollo.
Información y registros de Gestión de bromatología corporativa.
Gestión de Recursos Humanos e información de las actividades del área de compras.
Información del centro de distribución y de logística.

Servidor 4

Información involucrada a la producción: Control y Programación de la producción, control de producción.
Registros de los Servicios Centrales y del área de Sistemas.

Situación resultante:

Servidor 1

Información de Servicios asociados a la Producción: Oficina Técnica; Ingeniería; Mantenimiento mecánico y eléctrico; Servicios Centrales; Sistemas...

Servidor 2

Administración; Compras y Registros de consumos de materias primas e insumos.

Servidor 3

Se particionaron los discos del servidor para obtener tres recursos compartidos independientes cuyo uso se distribuyó según las siguientes funciones:

1. Carpetas y archivos del Sistema de Gestión Integral: gestión de los grupos autónomos y pilares del sistema.
2. Información de Investigación y Desarrollo. Gestión de bromatología corporativa.
3. Recursos Humanos, Capacitación y Seguridad Industrial.

Servidor 4

Información de todos los recursos directamente involucrados a la producción: programación de la producción, control de producción. Control y registros del sistema de Calidad (por ejemplo todos los registros de las normas ISO 9000).
Información de logística y movimientos del centro de distribución.

Objetivos logrados:

Se optimizó el espacio en disco priorizando los recursos que tienen mayor uso y criticidad.
Se colocaron en los mismos servidores carpetas afines para mayor comodidad de los usuarios, por ejemplo la información de Recursos Humanos, de Instructores y de Capacitaciones estaban alojadas en servidores diferentes.
Esto también permite que la expansión del uso de los recursos de algún grupo de usuarios no perjudique al de otros.

Tareas:

Se logró mediante la incorporación de un nuevo disco -aprovechando el presupuesto para ampliación y actualización de servidores-, y la reestructuración completa de las carpetas compartidas.
Tareas realizadas:
Recopilación de información y análisis de la situación.
Incorporación de la nueva unidad en el RAID de discos.
Reubicación de carpetas según criterio mencionado desde la estructura anterior a la actual (ver esquema anterior).
Todos los movimientos se hicieron cuidando que se conserven los permisos de usuarios y grupos de usuarios sobre los diferentes objetos.
Modificación y prueba de los diferentes script de conexión para que cada usuario y/o grupo de usuarios puedan seguir accediendo a la información de la misma manera que lo hacían hasta ahora.
Revisión del programa de backup para que ningún recurso quede sin el resguardo necesario.

6 - Controles aplicados en el Centro de Cómputos (Seg. Física):

Activo identificado como crítico	Referencia a la Norma IRAM-ISO 17799	Política de seguridad asociada	Riesgo efectivo	Riesgo esperado
Equipamiento en el Centro de Cómputos	7 Seguridad Física y Ambiental 8.4.1 Resguardo de la información 9.5 Control de acceso al sistema operativo	Uso aceptable Servidores	XX puntos	XX puntos

Tiempo efectivo de aplicación: a partir de Enero de 2005.

Modificaciones realizadas:

Se presupuestó y se aceptó la compra de dos racks con sistema de enfriamiento para la reubicación de los servidores. Se incluyó el cableado de energía con un nuevo tablero para asegurar los servicios en el caso de que falle la fuente de algún equipo. Cada servidor tendrá su llave de protección independiente. – Control de reducción de riesgos eléctricos.
(Ver fotos previas y posteriores a los cambios en el anexo 4)
Se incorporó un termómetro de ambiente y se reubicaron los matafuegos. – Reducción de riesgos ambientales.

Se redujo la oficina del referente de Tecnología Informática del sitio creando una sala de reuniones con puerta independiente y cambiando la puerta de acceso a los equipos para que sólo se pase al área restringida si se accede a la mencionada oficina. – Control de acceso físico.

Dado un inconveniente ocurrido (se quemó uno de los motores de los radiadores de refrigeración), se cambió la refrigeración de la sala haciendo ingresar el aire frío de las cañerías de enfriamiento de la planta al Centro de Cómputos. – Control de prevención de incendios.

Modificaciones previstas:

Se está en tratativas para cambiar la UPS con el propósito de aumentar el tiempo de servicio que brindan las baterías de la misma. Objetivo: mayor prevención ante cortes más prolongados de energía y actualización de la UPS existente.

Procedimientos.

Procedimiento para la configuración de seguridad en equipos de escritorio o móviles.

Con este procedimiento se enumeran todos los pasos a seguir con el objetivo de obtener un único instructivo de configuración; aún para los equipos nuevos. Si bien no en todos se utilizan todas las aplicaciones, bien sirve como guía.

- Instalar todos los parches de actualización adecuados según el sistema operativo que se encuentran en el servidor de instaladores.
- Asegurarse que el sistema de archivos sea NTFS para todas la unidades de disco, caso contrario convertirlo al mismo. "CONVERT unidad: /FS:NTFS"
- Siguiendo las siguientes referencias aplicar los permisos NTFS como se enumeran

  (Referencias: M=Modificar; L=Lectura; E=Escritura; X=Ejecución; FC=Control Total)

  Para el recurso:

  C:\

  Grupo local Administradores: FC

  System: FC

  Grupo local Usuarios: LEX

  Para los siguientes recursos se deben configurar los permisos para el grupo local Usuarios como se indica:

  C:\ LEX

  C:\Apind: M (Archivos temporales de aplicaciones industriales)

  C:\Spac: M (Archivos de trabajo del sistema de control de Calidad)

  C:\Archivos de Programa\Microsoft Office: M

  C:\Archivos de Programa\Archivos Comunes\Microsoft Shared: M

  C:\Archivos de programa\Archivos comunes\Network Associates: M (Antivirus)

  C:\Archivos de Programa\Reflection: M (Cliente para acceso a Main Frame)

  C:\Archivos de Programa\Citrix: M (Cliente para aplicaciones publicadas)

  C:\Archivos de Programa\Winamp: M

  C:\Archivos de Programa\iPass: M

  C:\Archivos de Programa\Corel: M

  C:\Archivos de programa\AutoCAD 2004: M

C:\Archivos de programa\Autodesk: M
C:\Archivos de programa\Network Associates: M (Antivirus)
C:\Archivos de programa\Windows Media Player: M
C:\Lotus: M (Cliente de correo electrónico)
C:\Windows (o WINNT): LEX
C:\Windows\System32 (o WINNT): LEX
C:\Windows\Temp (o WINNT): M
C:\Temp (si existe): M
C:\Windows\calidad.ini: M

Y sobre el registro de Windows también para el grupo local Usuarios modificar las siguientes claves como se indica:
HKEY_LOCAL_MACHINE\Software\Microsoft\Office: FC
HKEY_LOCAL_MACHINE\Software\Microsoft\Shared Tools: FC
HKEY_LOCAL_MACHINE\Software\Reflection: FC
HKEY_LOCAL_MACHINE\Software\Nullsoft: FC
HKEY_LOCAL_MACHINE\Software\iPass: FC

- Incorporar al usuario que utilizará el equipo al grupo local "administradores". (Luego se quitará de este grupo para que inicie sesión como simple usuario local.)
  Nota: algunas aplicaciones requieren que se inicien una vez con privilegios de administrador, por ejemplo: MS-Office XX, Cliente de Informix, Cliente de correo corporativo, etc.
- Iniciar las aplicaciones del ejemplo anterior y las que se requieran una vez con el usuario final del equipo con privilegios de "Administrador Local"
- Crear una cuenta de usuario local con privilegios de administrador (con nombre XXX y contraseña YYY) y registrar estos datos en la base de instructivos y procedimientos de Tecnología Informática. (Se sugiere la misma para todos los equipos.)
- Cambiar la contraseña de la cuenta de usuario administrador original y deshabilitarla.
- Deshabilitar las cuentas originales del equipo, por ejemplo la cuenta "invitado"
- Mediante el editor de políticas de grupo se restringir el uso de utilidades de configuración. Utilizar el comando "GPEDIT.MSC" para habilitar la plantilla especialmente configurada.
- Incluir en el grupo local Administradores las siguientes cuentas de usuario o grupo:
  Domain Administrators;
  AdministradoresCaroya;

La nueva cuenta de Administrador;

La cuenta de Administrador original.

- Si en el equipo se requiere que sólo se pueda iniciar sesión interactiva mediante el usuario final (además de los administradores locales y del dominio) se deben quitar del grupo local Usuarios todas las entradas que tenga y agregar la cuenta del usuario que se necesita:

  DOMINIO \ *usuario*; (agregar)

  NT AUTHORITY \ INTERACTIVE (quitar);

  NT AUTHORITY \ Usuarios Autentificados (quitar);

  Otros (quitar).

- Quitar del grupo local "administradores" la cuenta de usuario que utilizará el equipo.
- Probar que las aplicaciones necesarias del usuario funcionen correctamente.

Procedimiento de configuración de Access Points y Unidades Móviles.

Configuración de Access Points.

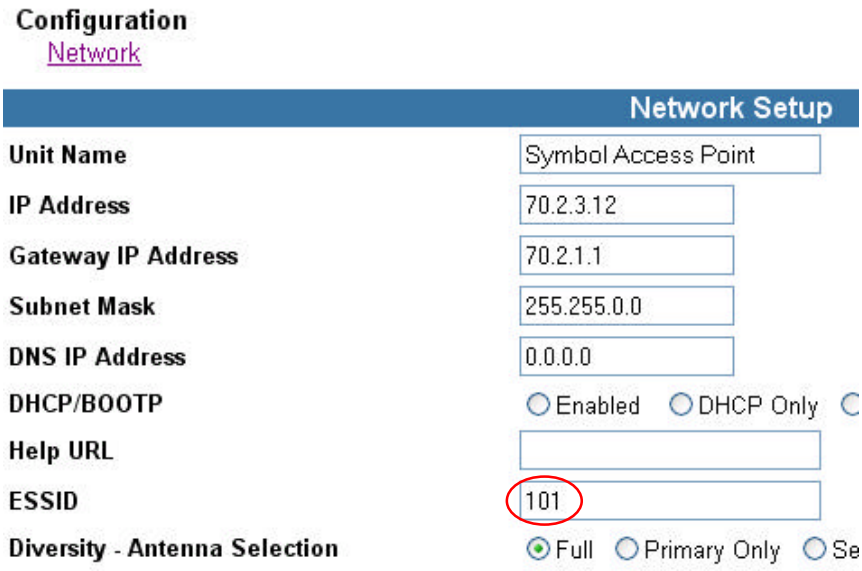
Consejo: Configurar primero las pantallas VRC y PDT antes que los Access Point (sino resulta muy complicado ingresar a los menús de configuración de los primeros).

Para tener un nivel aceptable de seguridad, básicamente se necesita hacer lo siguiente:

1. Cambiar la descripción por defecto que tiene la red inalámbrica.
2. Activar el filtro por MAC Address.
3. Activar la encriptación.
4. Cambiar el password de configuración que tienen por defecto los Access Points.

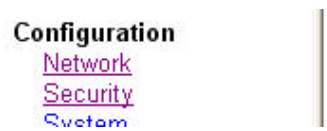
1. Cambiar la identificación de la red inalámbrica

En el menú "Network" del apartado "Configuration" se puede cambiar el nombre de la red inalámbrica. (ESSID)



Luego se debe salvar la configuración:

Las demás configuraciones de seguridad se encuentran en el menú "Segurity":



2. Control de acceso por MAC Address:

Los siguiente dos puntos trabajan en conjunto: hay que activar el control de Acceso y luego ingresar las MAC Address que se permitan conectar.

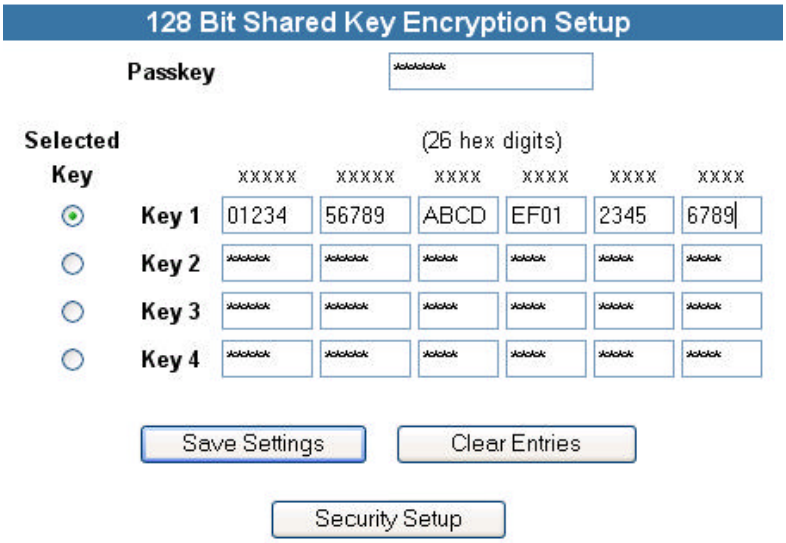
3. Activar la encriptación, cambiar el modo de encriptación y cambiar el key de encriptación:

Pantallas para la versión de Access Points **03.70-11**
(Más abajo se encuentras las indicadas para la versión: 03.92-08)

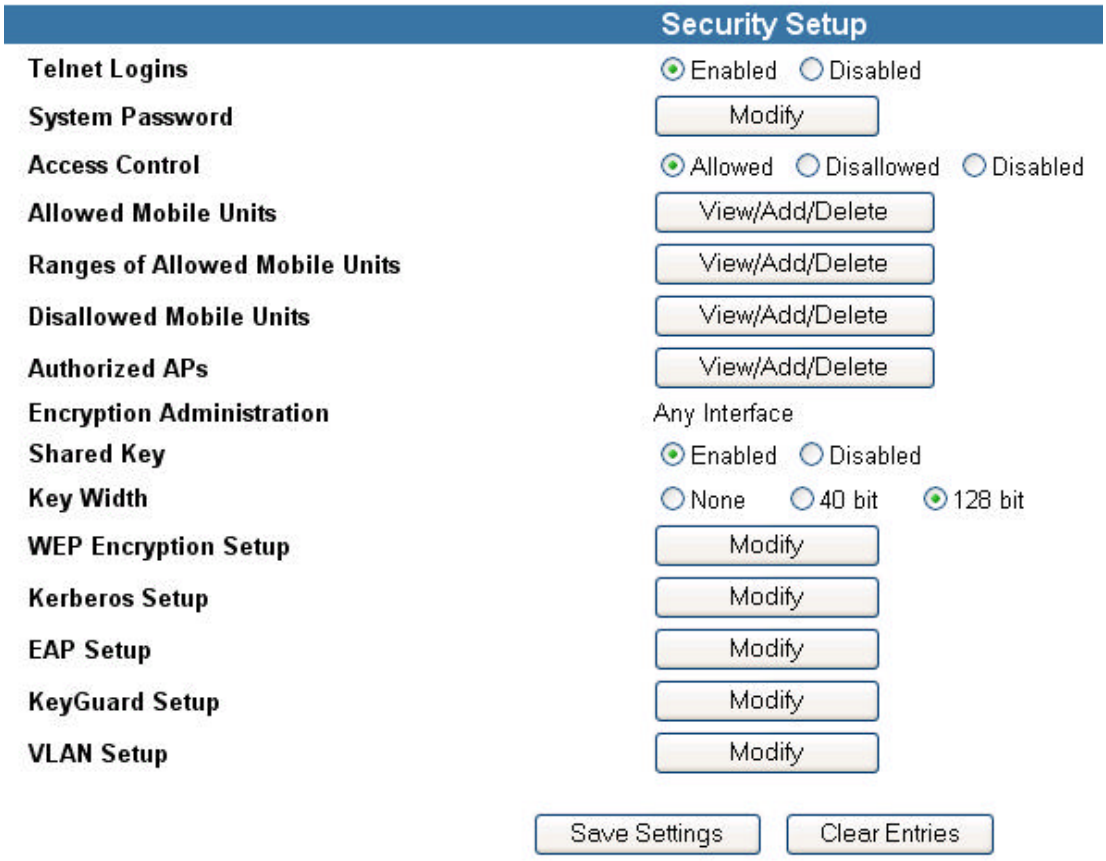
Seleccionar Enable en "Shared Key" y 128 bit en "Key Width".
Luego salvar la configuración para que permita ingresar a la pantalla de Keys correspondiente a la encriptación seleccionada.

Para introducir una llave de encriptación se puede agregar en PassKey (forma que no la soportan las pantallas VRC o PDT) o directamente en el Key que se seleccione: en el ejemplo en el 1.
Tanto el modo (128 bit), como el índice de Key (1) y el Key propiamente dicho (0123456789AB...) deben luego reflejarse en la configuración de los VRC o PDT.

Luego hay que salvar la configuración



Antes de salvar las configuraciones verificar que todo se vea así:

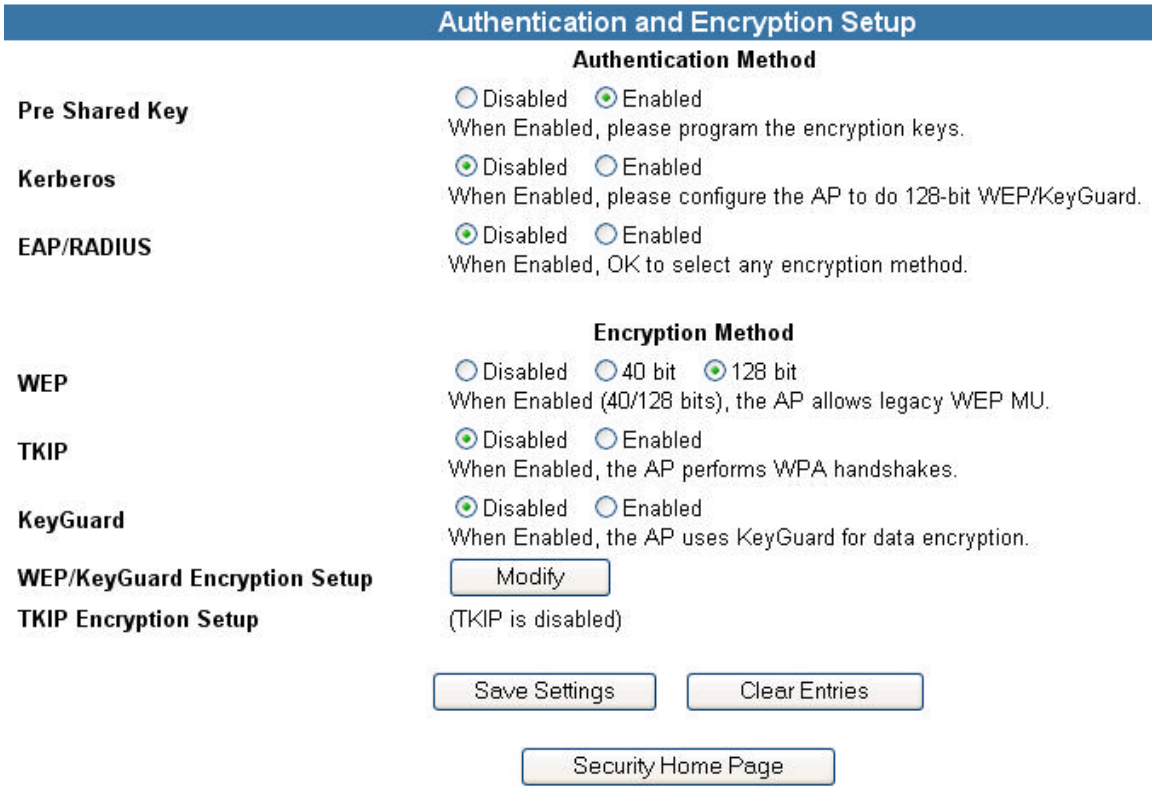


4. Para cambiar el password de acceso remoto:

Las pantallas de Encriptación para la versión de Access Points 03.92-08 son las siguientes:

Desde el menú "Security" ingresar a:

Luego de elegir en "Pre Shared Key" la opción Enabled se debe salvar la configuración y aparecerá el botón "Modify" que permitirá ingresar el Key de encriptación.



Configuración de pantallas VRC y PDT

Consejo: Configurar primero las pantallas VRC y PDT antes que los Access Point (sino resulta muy complicado ingresar a los menús de configuración de los primeros).

Ingreso al menú de configuración: Func + Ctrl + R
Password: SYSTEM

Contestar Yes (Y) a la pregunta
Warning: Any active session will be terminated. Continue? (Y/N)

Presionar la tecla 1: 1. Terminal Config

En ESS Id presionar Enter para cambiar el nombre de la red inalámbrica.

Luego ingresar al submenú Encryption:
Elegir el modo de encriptación en: Set Mode
Se debe elegir el mismo que se configuró en los Access Points (128 bits)
(No elegir 128 estándar)
Escribir la contraseña (números hexadecimales) en: Enter Keys
Colocar la misma que en el Access Point
Elegir el índice de Key correcto en: Set Key index
Elegir el mismo que en el Access Points (en el ejemplo el 1)

Salir de todos los menús con la secuencia de teclas CLEAR, ENTER y el número 3 según lo vaya solicitando.

Procedimiento de configuración de seguridad de un Servidor Windows 2000.

Backup full del servidor

Realizar un backup full del servidor. Considerar bajar los servicios Server, Informix, Domino (en los servidores que tengan instalados dichos servicios) y todos aquellos que sean innecesarios.

Salvar la configuración del servidor

Ejecutar la aplicación Administrador de Discos y guardar la configuración en un lugar diferente al servidor.

Ejecutar Windows NT diagnostics, ir a menú File, Print y seleccionar All tabs, Complete y guardar en un en una ubicación diferente al servidor.

Con el aplicativo "Dump Acl"

Realizar el seteo siguiente:

Report Permissions Report Options...

tildar las opciones SHOW OWNER, SHOW PERMISSIONS y SHOW ALL DIRECTORIES BUT NO FILES.

Los testeos o reportes a generar deben guardarse en archivos fuera del servidor. Estos son:

Permissions For Shares,

Dump Permissions For Files System (uno por cada disco desde la Raíz),

Permissions For Printers

Realizar discos de restauración.

Documentar la salida del comando " AT" para registrar las posibles tareas programadas.

Documentar la salida del comando "ipconfig /all"

Documentar NET START para conocer los servicios que se cargan automáticamente.

Respaldar el registro con "Save Key"

Revisión de componentes básicos

Verificar la instalación de los siguientes servicios en los servidores según su función:

En un servidor Miembro:

Alerter
BaanSCS Scheduler JobServer
BaanSCS Scheduler License Server
BrightStor Discovery Service
CA Backup Agent for Open Files
CA BrightStor Universal Agent
Computer Browser
EventLog
IECC Server Agent 3.0 - ol_mail
IECC VisiBroker 3.0 Osagent
Informix Dynamic Server - ol_mail
ISM Local Execution
ISM Portmapper
ISM Server
License Logging Service
Lotus Domino Server (LotusDominoData)
Messenger
Net Logon
Network Associates Alert Manager
Network Associates McShield
Network Associates Task Manager
Plug and Play
Protected Storage
Remote Procedure Call (RPC) Service
Schedule
Server
Spooler
TCP/IP NetBIOS Helper
TCP/IP Print Server
Workstation

Verificar la instalación de los siguientes software en los servidores

Client Config Snapin 3.0

Databases snapin 3.00

ER Administrative Tools

IMC & Snap-in Components

Informix Dynamic Server v7.30 (si corresponde)

Informix Storage Manager (si corresponde)

Lotus Domino (si corresponde)

McAfee NetShield

Microsoft Internet Explorer

Microsoft Windows Scripting Host

Schema Editors 3.00

Server Agent 3.0

Spaces Snap-in 3.00

SQL Editor 3.00 (si corresponde)

Deshabilitar y/o desinstalar el resto de los componentes

Deshabilitar los servicios que no figuren en el punto anterior.

Desinstalar los software que no figuren en el punto anterior.

Deshabilitar el servicio "Simple TCP/IP Services"

Ir a Panel de Control - Services y deshabilitar "Simple TCP/IP Services"

Revisión de Usuarios locales en los servidores Miembros

Los usuarios locales que deben estar en los servidores Miembros de los dominios, según las aplicaciones que tengan instaladas son:

Administrator

Guest

Informix (solo en los servidores que tengan motores Informix)

Usuario de arcSERVE backup (si fuera el servidor de backup)

Eliminar el resto de los Usuarios locales en los servidores Miembros

Eliminar los usuarios locales de los servidores Miembros que no figuren en el punto anterior.

Renombrar la cuenta Administrator del dominio local

Renombrar la cuenta Administrator como XXXXXX.

Deshabilitar la cuenta Guest del dominio local

Deshabilitar la cuenta Guest y colocarle una password.

Aplicación de políticas de usuarios de dominio a usuarios locales

Aplicar las política y directivas de contraseñas y cuentas de usuarios del Dominio a los usuarios locales.

Aplicar el último Service Pack disponible (al momento es SP4)

Verificar el espacio libre en el disco del sistema antes de instalar el SP.

Aplicar periódicamente las últimas actualizaciones de seguridad. Probarlas previamente.

Solucionar Null Session Admin Name

Ejecutar el Regedt32 y modificar el siguiente parámetro:

HKLM\System\CurrentControlSet\Control\LSA

Name: RestrictAnonymous

Type: REG_DWORD

Value: 1

Quitar permisos de edición remota del registro

Ejecutar el Regedt32 y configurar los permisos sobre cada una de las siguientes keys de esta forma:

Administrators - Full Control

Creator Owner - Full Control

Everyone - Read

System - Full Control

HKLM\SOFTWARE\Micrososft\Windows\CurrentVersion\Run
HKLM\SOFTWARE\Micrososft\Windows\CurrentVersion\RunOnce
HKLM\SOFTWARE\Micrososft\Windows\CurrentVersion\RunOnceEx
HKLM\SOFTWARE\Micrososft\Windows NT\CurrentVersion\AeDebug
HKLM\SOFTWARE\Micrososft\Windows NT\CurrentVersion\WinLogon
HKLM\SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg

Verificar el correcto funcionamiento y actualización automática del Antivirus

Verificar que el IIS y el Index Server no estén instalados

Desinstalar el IIS y el Index Server en los servidores.

Deshabilitar el IP forwarding

Deshabilitar el IP forwarding en los servidores.

Establecer mensaje de logon

Ejecutar el Regedt32 y modificar el siguiente parámetro:
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon
LegalNoticeCaption y escribir "Aviso Importante"
LegalNoticeText y escribir "Está prohibido el acceso no autorizado a este Servidor"

Modificar el valor de DCOM RunAs

Ejecutar el Regedt32 y modificar el siguiente parámetro:
HKLM\Software\Classes\AppID
Localizar la Key que tiene el valor "RunAs" y eliminar dicho valor

Modificar los permisos de las Key con el editor de la registry

Ejecutar el Regedt32 y configurar los permisos sobre cada una de las siguientes keys de esta forma:

Administrators - Full Control
Creator Owner - Full Control
Everyone - Read
System - Full Control

HKLM\Sosftware\Microsoft\Windows\CurrentVersion\
[App Paths | Control Folder | DeleteFiles | Explorer | Extensions | Ext ShellViews | Internet Settings | ModuleUsage | RenameFiles | Setup | SharedDLLs | ShellExtensions | Uninstall]

HKLM/Software/Microsoft/WindowsNT/CurrentVersion/
[Compatibility | Drivers | Drives.desc | Drivers32\0 | Embedding | MCI | MCI Extensions | Ports | ProfileList | WOW]

Sacar el grupo everyone del parámetro perlib

Ejecutar el Regedt32 y sacar el grupo everyone del siguiente parámetro:
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Perflib

Modificar seguridad NTFS.

Se debe aplicar la seguridad NTFS sobre las carpetas de los servidores siguiendo la siguiente guía:

Guía de configuración y administración de Seguridad de discos en Windows 2000 Server

Definiciones:

AdminBase:

Grupo Global de usuarios dentro del dominio que contiene a los administradores de la Base Operativa o los soportes locales de esa base o planta.

Usuarios Aplicación:

Grupo Global dentro del dominio que contiene a todos los usuarios que deben tener acceso a determinada aplicación.

Usuarios Base:

Grupo Global dentro del dominio que contiene a todos los usuarios de una misma base o planta de Arcor.

UsuarioX:

Perfil de usuario de una determinada persona.

GrupoX:

Grupo Global dentro del dominio que contiene a todos los usuarios que necesitan compartir determinado conjunto de archivos.

Pasos del Procedimiento:

1. Para la partición primaria "C:" debe existir un solo recurso compartido (Sharing) que es el "C$", tal como queda instalado por defecto para propósitos administrativos. Se debe eliminar el Sharing administrativo "Admin$" que comparte el recurso "C:\WINNT"
"AutoShareServer" (con tipo REG_DWORD y valor 0) en la key
HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters.

2. Para setear la seguridad NTFS de cada una de las carpetas de la unidad "C:" se debe tener en cuenta no utilizar al grupo "Everyone" para la asignación de la seguridad y sí, la aplicación de los siguiente criterios:

Reemplazar para los subdirectorios
C:\
Administrators -> Full Control
Backup Operators -> Change
System -> Change
Creator Owner -> Full Control
AdminBase / Authenticated users -> Read

En forma Individual
C:\WINNT\system32\regedt32.exe
Administrators -> Full Control
System -> Full Control

C:\WINNT\regedit.exe
Administrators -> Full Control
System -> Full Control

C:\WINNT\system32\config
Administrators -> Full Control
System -> Full Control
Creator Owner -> Full Control

C:\WINNT\repair
Administrators -> Full Control
System -> Full Control

C:\WINNT\system32\spool
Administrators -> Full Control
Backup Operators -> Change
System -> Change
Creator Owner -> Full Control
Everyone -> Read

3. La partición "D:" se debe asignar a la unidad de CD-ROM y la misma no debe compartirse como recurso de red.

4. También debe existir la unidad lógica o partición de datos, la misma debe ser denominada "F:", la misma se debe configurar de un tamaño igual al resto del espacio no utilizado por la partición anterior, y dependerá de la configuración física de los discos del servidor. La finalidad de esta única unidad por servidor es que sea el contenedor de todos los datos importantes de la empresa.

Para las particiones de datos se debe tener en cuenta la siguiente política de recursos compartidos.

Función del Servidor	Definiciones al Respecto
Database Server	No debe existir Sharing
Notes Server	No debe existir Sharing
File Server de Instaladores de Software	Se debe compartir solamente la carpeta que contiene el software para Instalar. Esta carpeta se debe llamar "Soft" y se debe desprender del directorio raíz del disco F: Ej: "F:\SOFT" La seguridad en el sharing debe estar dada de la siguiente manera: - Administrators ----------> Full Control. - Admin Base----------> Full Control.
File Server de Archivos de Usuarios	Se debe compartir solamente una carpeta que será de la que se desprenden las subcarpetas en donde se encuentran los archivos de los usuarios. Esta carpeta se debe llamar "Users" y se debe desprender del directorio raíz del disco F: Ej: "F:\USERS" La seguridad en el sharing debe estar dada de la siguiente manera: - Administrators ----------> Full Control. - Admin Base ----------> Full Control. - Usuarios Base ----------> Change.
File Server de Archivos de grupos de Usuarios	Se debe compartir solamente una carpeta que será de la que se desprenden las subcarpetas en donde se encuentran los archivos de los usuarios. Esta carpeta se debe llamar "Groups" y se debe desprender del directorio raíz del disco F: Ej: "F:\GROUPS" La seguridad en el sharing debe estar dada de la siguiente manera: - Administrators ----------> Full Control. - Admin Base ----------> Full Control. - Usuarios Base ----------> Change.

Se debe setear la seguridad NTFS de las carpetas de la unidad "F:" teniendo en cuenta de no utilizar para asignar dicha seguridad al grupo "Everyone", se debe realizar a partir de la raíz del volumen, siguiendo el siguiente criterio:

F:\
Administrators -> Full Control
Backup Operators -> Change
System -> Change
AdminBase -> Read

y aplicar a todos los directorios en forma recursiva
F:\LOTUS
Administrators -> Full Control
Backup Operators -> Change
System -> Change
AdminBase -> Change

y aplicar a todos los directorios en forma recursiva
F:\SOFT
Administrators -> Full Control
Backup Operators -> Change
System -> Change
AdminBase -> Change

No aplicar a los Subdirectorios
F:\USERS
Administrators -> Full Control
Backup Operators -> Change
System -> Change
AdminBase -> Change
Usuarios Base -> Read

F:\USERS\USUARIOX
System -> Change
UsuarioX -> Change

F:\GROUPS
Administrators -> Full Control
Backup Operators -> Change
System -> Change
AdminBase -> Change
Usuarios Base -> Read

F:\GROUPS\GRUPOX
Administrators -> Full Control
Backup Operators -> Change
System -> Change
AdminBase -> Full Control
GrupoX -> Change

Procedimientos recomendados para Anti-virus

Procedimientos recomendados para prevenir inconvenientes con virus:

- ?? Siempre se debe ejecutar el software antivirus corporativo dado que se posee licencias, soporte y está garantizada la actualización periódica.
- ?? Nunca se deben abrir archivos o macros anexadas a correos electrónicos de origen desconocido o sospechoso. Borre dichos archivos y/o correos.
- ?? Borre spam, cadenas y cualquier correo electrónico basura sin reenviarlos.
- ?? Nunca baje archivos desde sitios de Internet desconocidos o sospechosos.
- ?? Evite compartir recursos de su PC con accesos de lectura y escritura a menos que sea absolutamente necesario para sus tareas laborales.
- ?? Siempre examine cualquier medio extraíble, de origen desconocido, antes de su uso a fin de asegurarse que esté libre de virus.
- ?? Realice respaldos de datos críticos y configuraciones de sistemas y almacene el medio en un lugar seguro.
- ?? Si por algún motivo el software anti-virus no esté activo, no ejecute ninguna aplicación que pueda transferir virus, por ejemplo: compartir archivos o el correo electrónico.

Planes de contingencia.

Plan de contingencia ante extravío, robo o rotura de equipos móviles críticos.

Ante un inconveniente de envergadura como los indicados, se posee una PC móvil con todo el software -instalado y probado- que necesita cualquier directivo.
Dicha PC también podrá ser utilizada en el caso de tener que tramitar alguna garantía.
Las características del equipo de backup son las necesarias para suplir cualquier otro equipo que entre en emergencia: velocidad de procesador, memoria instalada, adaptador gráfico adecuado. También posee las interfaces de conectividad necesarias.
Se prevé que dicho equipo se utilice únicamente para éste motivo de modo que, llegado el caso, esté disponible y operativo.

Los pasos a seguir ante un evento son:

- Configurar el equipo de backup con el entorno funcional y gráfico adecuado a la persona.
- Restaurar la información personal de dicha persona desde el servidor de Backup.
- Configurar la seguridad local del equipo como está indicado en el "Procedimiento para la configuración de seguridad en equipos de escritorio o móviles".
- Comprobar que el interesado pueda acceder a los recursos que necesita: sistemas; carpetas locales, información en servidores; impresoras locales y de red.
- En caso de robo o extravío solicitar al usuario que haga la denuncia pertinente.
- En caso de desperfecto o rotura de alguna parte se deberá realizar la solicitud de servicio técnico mediante los canales habilitados para tal fin: registro de un incidente en el sistema especialmente desarrollado.
- Solicitar la autorización de la Gerencia de Tecnología Informática para la adquisición de un nuevo equipo.
- Solicitar a la gerencia que corresponda la compra fuera del presupuesto anual.
- Tramitar la baja del bien de uso del sistema administrativo de Activos Fijos bajo la causa adecuada: robo, extravío, rotura, etc.
- Generar la baja correspondiente del inventario de hardware.

Plan de contingencia ante desperfectos en equipos de la red inalámbrica.

Para el desperfecto de algún equipo de la red inalámbrica (Access Points o Unidades móviles) se cuenta con un backup para cada tipo de dispositivo.
Dichos equipos se han probado adecuadamente y se encuentran configurados y operativos con el simple hecho de encenderlos.

Ante un inconveniente se deben seguir los siguientes pasos:

- Instalar el equipo de reemplazo que corresponda y asegurarse que quede en óptimas condiciones durante el tiempo que haga falta hasta que se repare o reemplace el equipo defectuoso.
- Realizar la solicitud de servicio técnico: registro de un incidente en el sistema correspondiente.
- Si el dispositivo quedara en desuso:
  - se debe solicitar la autorización de la Gerencia de Tecnología Informática para la adquisición de un reemplazo.
  - se debe solicitar a la gerencia correspondiente la compra del equipo no presupuestado.
  - tramitar la baja del bien de uso del sistema administrativo de Activos Fijos bajo la causa de baja por desperfecto.
  - generar la baja correspondiente del inventario de hardware.

Conclusión.

Recordando lo dicho en la introducción: “Espero que este esfuerzo constituya un buen punto de partida para la reflexión y el debate sobre esta problemática (de la seguridad informática) en la organización”; puedo resaltar ahora que mis expectativas sobre este trabajo fueron cubiertas ampliamente.

El esfuerzo no sólo ha contribuido positivamente en la empresa, dado que se han tomado acciones concretas aún más allá del alcance del trabajo; sino que además se ha ganado en concientización sobre la seguridad y cuidado de la información. Muchas personas se han involucrado activamente interesándose o colaborando directamente, contestando encuestas, generando propuestas de políticas y hasta sugiriendo que el tema de la *confidencialidad, integridad y disponibilidad de la información* debe incluirse en la Política General del Sistema de Gestión Integral del grupo ARCOR.

Muchos, simplemente se han interesado.

En todo me he sentido gestor de esa conciencia y muy a gusto, por cierto, con el bagaje de conocimientos adquiridos.

Además toda esta actividad (consultas, encuestas, comentarios a cerca del trabajo, análisis), trajo aparejado logros y reconocimiento en la empresa que se traducen en responsabilidades recibidas más allá del ámbito de la planta industrial de Colonia Caroya.

Siento la obligación de resaltar que, siendo el tema del presente trabajo sumamente amplio, el abanico de posibles respuestas a las preguntas: ¿ahora qué?; ¿cómo continuamos? en mi opinión no tiene límites; y en cambio invita a abrir otras puertas que en principio compartirían gran parte del mismo escenario.

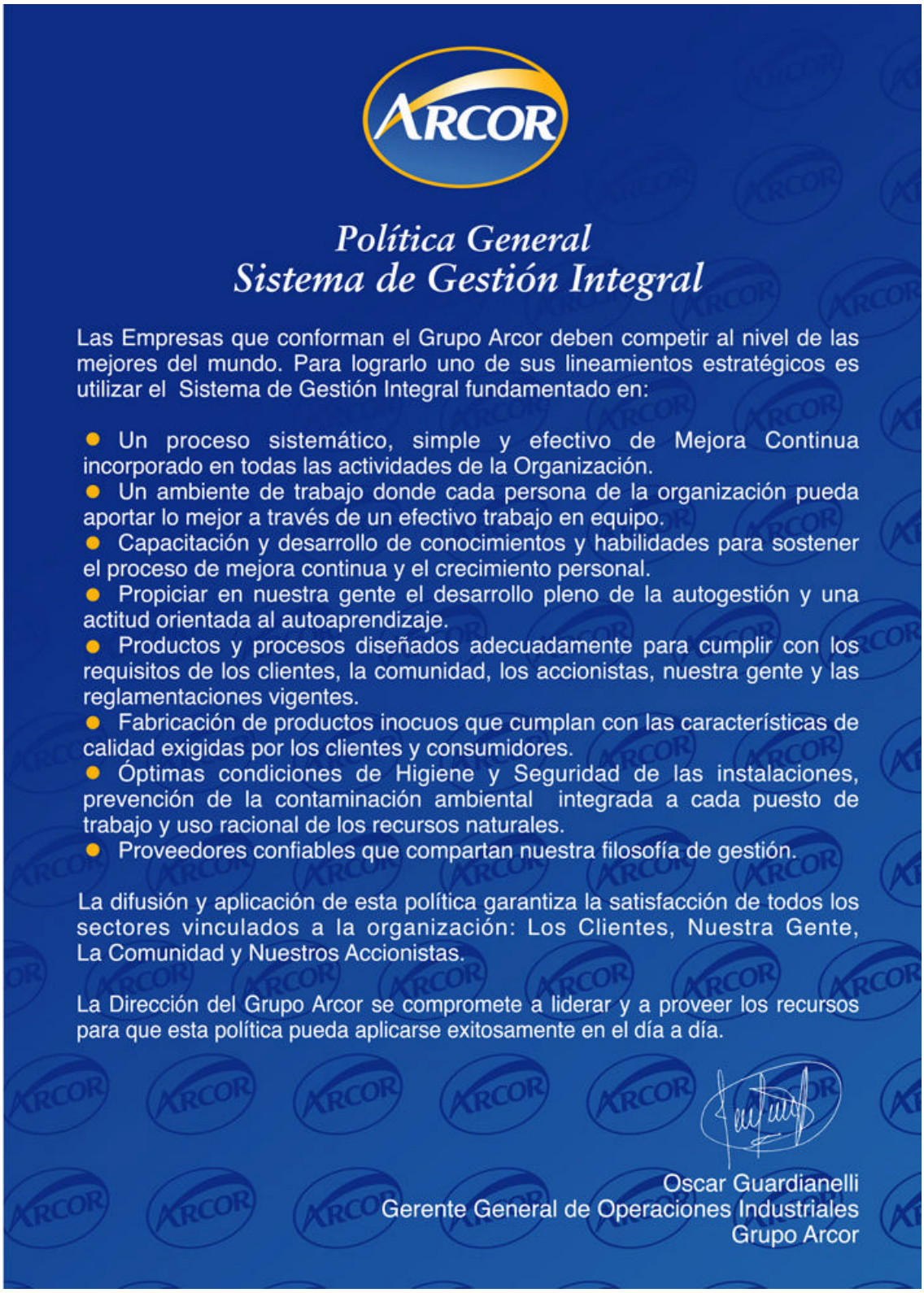
Me atrevo a interpretar que el desafío está en la continuidad: lograr con el grupo de Seguridad Informática de Arcor un esquema básico que permita hacer análisis de riesgo de seguridad periódico y con personal interno. Y que se pueda replicar en otras bases de Arcor.

Implicará por cierto seguir profundizando el presente análisis y la aplicación de más métodos técnicos que mejoren el acercamiento a la realidad.

El nuevo objetivo será que el área de Tecnología de la Información continúe como soporte de las actividades productivas y asegure, desde el ámbito de su competencia, la continuidad de las operaciones del Grupo ARCOR.

En un marco más general, la incorporación de la seguridad informática como un aspecto constitutivo del Sistema de Gestión Integral de la compañía, sobre el que se asuma el compromiso de la mejora continua desde la organización en su conjunto, es un horizonte que ya se vislumbra en el presente.

Anexo 1 (Política del Sistema de Gestión Integral – S.G.I.)



ARCOR

Política General
Sistema de Gestión Integral

Las Empresas que conforman el Grupo Arcor deben competir al nivel de las mejores del mundo. Para lograrlo uno de sus lineamientos estratégicos es utilizar el Sistema de Gestión Integral fundamentado en:

- Un proceso sistemático, simple y efectivo de Mejora Continua incorporado en todas las actividades de la Organización.
- Un ambiente de trabajo donde cada persona de la organización pueda aportar lo mejor a través de un efectivo trabajo en equipo.
- Capacitación y desarrollo de conocimientos y habilidades para sostener el proceso de mejora continua y el crecimiento personal.
- Propiciar en nuestra gente el desarrollo pleno de la autogestión y una actitud orientada al autoaprendizaje.
- Productos y procesos diseñados adecuadamente para cumplir con los requisitos de los clientes, la comunidad, los accionistas, nuestra gente y las reglamentaciones vigentes.
- Fabricación de productos inocuos que cumplan con las características de calidad exigidas por los clientes y consumidores.
- Óptimas condiciones de Higiene y Seguridad de las instalaciones, prevención de la contaminación ambiental integrada a cada puesto de trabajo y uso racional de los recursos naturales.
- Proveedores confiables que compartan nuestra filosofía de gestión.

La difusión y aplicación de esta política garantiza la satisfacción de todos los sectores vinculados a la organización: Los Clientes, Nuestra Gente, La Comunidad y Nuestros Accionistas.

La Dirección del Grupo Arcor se compromete a liderar y a proveer los recursos para que esta política pueda aplicarse exitosamente en el día a día.

Oscar Guardianelli
Gerente General de Operaciones Industriales
Grupo Arcor

IMPLEMENTACIÓN DEL SGI

La División Chocolates del Grupo Arcor S.A.I.C. ha logrado alcanzar el liderazgo en el Mercado Interno a través de un fuerte desarrollo de nuevas tecnologías, equipamientos y políticas de comercialización que le permiten proyectar este crecimiento al ámbito regional, a la vez que ganar nuevos mercados internacionales. El contexto en que se dio este crecimiento se torna cada vez mas agresivo (apertura del mercado, globalización), lo que nos impone mejorar cada día mas y mas rápidamente nuestros estándares apuntando al liderazgo de costos y a la innovación, o sea, nuestra competitividad.

Para lograr estos objetivos, industrialmente, surge que debemos focalizarnos en acelerar los procesos de mejora continua para:

Aumentar la flexibilidad de las líneas de producción, los índices de calidad, disminuir drásticamente las pérdidas y desvíos de consumo, devoluciones de clientes e indisponibilidad de equipos, asociados a un incremento en los niveles de limpieza, seguridad y cuidado del medio ambiente de las plantas.

Estos objetivos concretos y su logro están alineados con la misión de nuestro negocio que es .....

... ***"responder a las necesidades de gratificación de niños, jóvenes y adultos a través de productos de y con chocolate, masivos e industriales que cumplan standards de calidad internacional, cub riendo todos los segmentos socioeconómicos y sin limitaciones geográficas"*** y el lema corporativo ***"Calidad que conviene"***

Para lograrlo debemos adoptar necesariamente una nueva herramienta de gestión que integre a todos los niveles de la compañía, promoviendo una cultura más participativa y una alta motivación en toda la organización, significando un cambio cultural que tenga como eje central la **Mejora Continua,** optimizando los procesos productivos y adoptando una constante capacitación y entrenamiento, tendiendo a cero las pérdidas, los defectos y los accidentes.

El compromiso de todo el personal para establecer este sistema, como es el Sistema de Gestión Integrado ARCOR, tiene el respaldo en el compromiso formal que aquí asume la Gerencia General del Negocio en apoyar y sostener con todos los recursos necesarios, la implementación del mismo en la Planta de Chocolates de Colonia Caroya.

Guillermo Storni
Gerente General División Chocolates
Julio del 2000.

Anexo 2 (Replicación de seguridad en redes inalámbricas)

Correo electrónico de conformidad con los procedimientos probados para aplicar seguridad en las redes inalámbricas del centro de distribución de ARCOR en Colonia Caroya. Se invita a realizar un documento con dichos procedimientos para establecerlo como procedimiento en las bases de Arcor que tengan dicha configuración ya sea en país o fuera del mismo.

(Están ocultos los nombres del Gerente de Seguridad Informática del Grupo; del Gerente de Tecnología Informática y Comunicaciones y del referente del soporte técnico local de ARCOR Caroya)

[redacted]
08/04/2005 03:44 PM

Para: [redacted]R/Arcor@Arcor, Guillermo Young/Caroya/AR/Arcor@Arcor
cc: [redacted]/Arcor@Arcor
Asunto: Re: Fw: Seguridad en Access Point

[redacted] Guillermo,

el tema de Seguridad hace todos, no solo al área específica, con esto quiero decir que es correcto lo que hicieron y no duden en hacerlo de nuevo con otros temas.

La configuración que probaron es correcta, deberían preparar un documento con el detalle, luego lo estableceremos como procedimiento y haremos extensivo a todas la instalaciones donde tengamos Access Point dentro o fuera del país.

Quedo a disposición para cualquier consulta.

Saludos,

[redacted]
Gerente de Seguridad Informática
Grupo Arcor
Tel.: [redacted]

[redacted]ito/AR/Arcor

[redacted]rroyito/AR/Arcor
08/04/2005 11:48 a.m.

To [redacted]R/Arcor@Arcor
cc [redacted]/Arcor@Arcor, Guillermo
Subject Fw: Seguridad en Access Point

[redacted]

la última vez que estuve en Caroya encontramos con Guillermo Young y [redacted] que desde las oficinas cercanas al Centro de Cómputos podíamos engancharnos a la LAN en forma inalámbrica. Como el CD se está extendiendo hacia el lado de la ruta, esto podría llegar a convertirse en una falla de seguridad, considerando además que enganchándonos en forma inalámbrica le restamos performance a las RF's del Centro de Distribución.

Por tal motivo y aprovechando los conocimientos de Guillermo sobre la instalación RF de Caroya, le pedí que investigara el tema, llegando a la conclusión que a continuación te remito. Sin intentar inmiscuirnos en tus temas, creo que habría que considerar esto no solamente en Caroya sino en todos los CD's donde tenemos RF de esta tecnología. Un capítulo a investigar sería en [redacted], donde tenemos tecnología propietari[redacted].

Por favor contá con nosotros para lo que necesites.

Saludos
[redacted]

----- Forwarded by [redacted]rroyito/AR/Arcor on 08/04/2005 11:31 a.m. -----

Guillermo Young/Caroya/AR/Arcor
08/04/2005 09:46 a.m.

To [redacted]rroyito/AR/Arcor@Arcor
cc
Subject Seguridad en Access Point

[redacted]

Cómo sabés, encontramos una falla de seguridad en los access point del centro de distribución.
Configurados como están (de fábrica) cualquier pc con red inalámbrica habilitada puede ingresar a la red de Arcor.

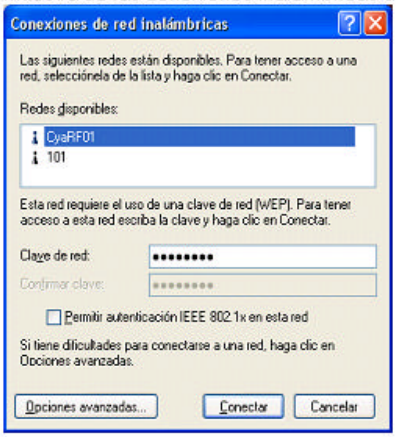
Por ese motivo he hecho algunas pruebas con los access point que tengo para la ampliación.

- Cambié la clave de configuración que viene por defecto para la administración de los access point vía Telnet
- Cambié el nombre por de defecto de la red inalámbrica 101 por [redacted]
- Habilité la encriptación con contraseña de 128 bits
- Habilité el filtro por MAC address

Hice las pruebas pertinentes con resultados positivos.
Tanto las notebooks como los VRC se pudieron conectar (previa configuración de la clave)
Me falta ver que los access point no publiquen el nombre de la red inalámbrica.

Si te parece bien, hago un programa para implementarlo en el entorno de producción.

Muestra de las conexiones inalámbricas disponibles (durante las pruebas)



Otras opciones de seguridad más complejas no están disponibles en los VRC.
Por ejemplo las de autenticación, etc.

Saludos,

Guillermo Young
Tecnología Informática
Grupo ARCOR - Argentina

Correo electrónico del Gerente Seguridad Informática agradeciendo el aporte.

[redacted]
27/04/2005 11:13 AM

Para: Guillermo Young/Caroya/AR/Arcor@Arcor
cc: [redacted]rroyito/AR/Arcor@Arcor
Asunto: Re: Seguridad en Symbol

Guillermo,
está muy bien y claro el procedimiento, lo publicaremos al resto de las bases.

Desde ya muchas gracias por tu aporte.

Saludos,

[redacted]
Gerente de Seguridad Informática
Grupo Arcor
Tel.: ([redacted]
Guillermo Young/Caroya/AR/Arcor

Guillermo Young/Caroya/AR/Arcor
12/04/2005 07:30 p.m.

To [redacted]to/AR/Arcor@Arcor, [redacted]u/AR/Arcor@Arcor
cc
Subject Seguridad en Symbol

[redacted]
He agregado en el manual de procedimientos e instructivos correspondiente una primera versión del procedimiento a seguir para asegurar la red inalámbrica Symbol.

PROCEDIMIENTO *PG1127* *Procedimien*

Nombre del Procedimiento: Symbol - Configuración de Seguridad de la red inalámbricas **Estado:** Vigente

Categoría: Seguridad **Alcance:** Tecnología Informática

Fecha de creación: 12/04/2005

Descripción:

Seguir el siguiente procedimiento para asegurar la red inalámbrica de Symbol a un nivel más que aceptable.

Procediminto de Seguridad para RF.doc

Correo electrónico del Gerente de Seguridad Informática enviando el estándar de configuración de Access Point al resto de las plantas de Arcor. Se envía a todos los soportes técnicos locales y se copia al Gerente General de Sistemas, al Gerente de Tecnología Informática y comunicaciones corporativo y al resto del Grupo de Seguridad Informática.

[redacted]
27/04/2005 11:24 AM

Para: [redacted]

cc: [redacted]

Asunto: Estándar de seguridad para Access Points

Estimados,

les envío el estándar para la configuración de los Access Points que deberán aplicar en todas las instalaciones que tengan en sus respectivas bases.

Dicho estándar fue realizado por Guillermo Young, al que le agradezco su participación, y aprobado por la Gerencia de Seguridad Informática.

Procediminto de Seguridad para RF.doc

Quedo a disposición para cualquier consulta.

Saludos,

[redacted]
Gerente de Seguridad Informática
Grupo Arcor
Tel.: [redacted]

Anexo 3 (Encuesta a usuarios – consolidación.)

Identificación de activos desde la necesidad concreta de usuarios clave por sectores. El trabajo se realizó tomado como base la encuesta sugerida por OCTAVE para el personal en general.

En la página siguiente se presentan las preguntas de la encuestas consolidadas.
Luego están consignadas:

- las conclusiones de los **activos** identificados por los usuarios ;
- las **amenazas** y **debilidades** enumeradas y;
- las conclusiones de las **preguntas abiertas** y **cerradas** por tópicos.

Consulta a usuarios CONSOLIDADA

Activos importantes
Describa brevemente todas las actividades que se realizan en su sector en las que se utilicen equipos informáticos.
Ingeniero de procesos: *Seguimiento de prototipos; *seguimiento de proyectos; *análisis de indicadores y pérdidas; *análisis de información de gestión industrial (JDE); *consultas de SPAC.
Control de producción: *One-World; *Sifab; *Carh; *Lotus; *Fondo fijo; *Business Objects; *Mantec; *Planillas electrónicas (Tablero de comando; Indisponibilidad); *Costos; *Análisis varios de control de producción; etc.
Medio Ambiente, Higiene y Protección Industrial: *Registro y estadísticas de accidentes; *Registro y estadísticas de control de plagas; *Registro y estadísticas de Tarjetas de Incidentes; *Tratamiento sistemático de problemas; *Auditorias; *Legislación aplicable; *Registro y estadísticas de residuos sólidos; *registro y estadísticas de efluentes líquidos; *Registro de mediciones de higiene. *Registro en hojas de revisión de elementos de seguridad; *Procedimientos; *Material de capacitaciones en seguridad; *Planillas de permisos de trabajo; *Planillas de stock de indumentaria del personal; *Registros de limpieza; *Registros de aparatos sometidos a presión; *Registros de emanaciones gaseosas.
Administración de Mantenimiento y Oficina Técnica: *Administración de recursos (materiales y mano de obra); *Realización/impresión de reportes para mantenimiento preventivo; *Manejo de información técnica (planos, manuales, instructivos, etc.)
Administración de materiales productivos: *Se verifican necesidades de Materiales Productivos, sus consumos. Se pasan órdenes de compra por correo y luego se activan telefónicamente.
Instructores del SGI.: *JDE: Pedidos de compras de materiales auxiliares; *pedidos al almacén; *Excel, PowerPoint, Word, Paint, Editor Fotográfico, AutoCad; *Internet; *Lotus; *Módulo de tarjetas (TPM); *Fondo Fijo; *Scanneos, Impresiones color y b/n; *Carh; *People Soft.
Gestión de Calidad: *Inspección (aprobación / rechazo) de insumos (materia prima y materiales de empaque); *Compra de insumos de laboratorio (reactivos, descartables, etc.), librería (stickers de identificación de estado), etc.; *Control de proceso (estadísticas de variables y atributos); *Control de producto; *Cálculo de Indicadores (reclamos, producto No conforme, índices de calidad); *Check de cumplimiento de condiciones en base a especificaciones.
**Gerente corporativo de Gestión de Calidad: ***Correo electrónico; *Documentos en Word, Excel, PowerPoint (creación y almacenamiento); *Aprobación de compras; *Consultas de Internet; *Consulta / búsqueda de información en Servidores.
Compras: *Procesamiento de datos para gestión de compras (y almacenamiento) (utilitarios); *Comunicaciones internas y con proveedores vía correo electrónico; *Búsqueda de información en Internet; *Seguimiento del mercado del Cacao (sistema CMA); *Emisión de pedidos de compra (JDEwards); *Seguimiento de evolución de indicadores (Business Objects); Elaboración de estadísticas relativas a compras (JDE).
Jefe del Centro de Distribución: *Control de Warehousing en todo el Centro de Distribución (Ingreso y egreso de mercadería, confirmación de productos terminados en almacenamiento. Confirmación de pedidos, créditos, devoluciones prebalanceo y balanceo de carga. Facturación.
Jefe de Investigación y Desarrollo: *Administración de Prototipos; *Confección de Especificaciones; *Seguimiento de Proyectos; *Inscripción Bromatológica.

?? ¿Cuáles son los activos más importantes que deben asegurarse en su sector?

Activo (Enumérelos abajo)	**Impor-tancia** (1 poca, 5 mucha)	Qué tipo de seguridad se requiere para cada activo.			**Debilidades** de cada activo.	Posibles **Amenazas** sobre cada activo.
		Disponi-bilidad (1 poca, 5 mucha)	**Integridad** (1 poca, 5 mucha)	**Confiden-cialidad** (1 poca, 5 mucha)		
Información nuevos proyectos	5	5	5	5	ns/nc	divulgación
Historial de proyectos	5	5	5	5		Ídem
PC – impresora	5	2	-	-		
Historial propio	5	5	5	5	No tengo backup	Cualquiera puede acceder a la PC
Spac / JDE / Notes	5	4	5	4		
Información: estructura de productos	5	5	5	5		
Sistemas / software: costos; balance de masa	5	5	5	2	Lentitud	
Personas (confidencialidad)	4	5	5	5		
Información en el Servidor	5	5	5	5		
Programa de legislación	4	5	5	2		
Impresora láser	5	5	5	4	Insumos	
Impresoras injet	3	3	4	3		
PC's	4	5	5	5	No hay backup de discos locales	Virus / accesos externos
Operador (personal)	5	5	5	5		Manejo de la información
Información en servidores	5	5	5	5		
Personas	5	4	5	5	Estancamiento	Traspasos
Información	4	5	5	5	Desactualización	Filtraciones
Software	4	5	4	4	Fallas	
PCs	5	5	5	2	Lentitud	Aumento de archivos "pesados"
Impresora	4	5	3	1	Desconfiguración	
Información en servidores	5	5	3	3	Saturación	Imposibilidad para guardar información
Spac	5	4	5	2	Indisponibilidad en turnos noche	
JDE	3	4	5	2	Bloqueos de usuarios	
Información en servidores	5	5	5	4	Poco espacio en los servidores	
Doc9000	5	5	5	2	Actualización de usuarios	
Sistema de especificaciones de productos	5	4	5	3		

?? ¿Cuáles son los activos más importantes que deben asegurarse en su sector?

Activo (Enumérelos abajo)	**Importancia** (1 poca, 5 mucha)	Qué tipo de seguridad se requiere para cada activo.			**Debilidades** de cada activo.	Posibles **Amenazas** sobre cada activo.
		Disponibilidad (1 poca, 5 mucha)	**Integridad** (1 poca, 5 mucha)	**Confidencialidad** (1 poca, 5 mucha)		
Fichas de reclamos de consumidores (desde '95)	4	3	5	3	Copia papel sin resguardo	
Carpeta de validación de PCC y HACCP	5	4	5	3		
SGI (manuales, procedimientos, instructivos)	5	5	5	2		
PCs del sector	5	5	5	3	Información local de estudios HACCP y diagramas de flujo	
Correo electrónico	2	4	5	4	Posibilidad de acceso a la base	Personas internas de la organización
Documentos (PowerPoint / Word / Excel)	4	4	5	4	Que la información pueda ser borrada por alguna mala maniobra propia.	Yo, al ser administrador de estos documentos.
Notebook	3	5	4	4	Pérdida / robo	Robo por terceros en viajes o que ingresen a la oficina.
Documentos en servidores	2	3	3	3	Perdida de información por falta de backup / réplicas de mail hechas, etc.	Accesos por personas no autorizadas
El propio conocimiento	5	5	4	5		
Personal área de compras	5	4	5	5	Vulnerabilidad; Falta de conocimientos sobre seguridad; Falta de actitud hacia el cuidado de activos.	Acción de competidores; Prácticas deshonestas de proveedores; Eventos accidentales por las personas u otros factores.
Información (archivos en discos locales incluyendo réplicas de correo; archivos físicos y en carpetas)	5	5	5	5	Sin protección física adecuada; Sin copia de seguridad; Libre acceso de otros usuarios al Server; Mal archivada (físico o virtual); Dificultad p/acceso rápido.	Pérdida por descuidos propios o de terceros; Modificación de datos accidentalmente o no, por personas dentro o fuera de la organización. Pérdidas de tiempo por búsqueda o reconstrucción.

(continuación...)

?? ¿Cuáles son los activos más importantes que deben asegurarse en su sector?

Activo (Enumérelos abajo)	**Importancia** (1 poca, 5 mucha)	Qué tipo de seguridad se requiere para cada activo.			**Debilidades** de cada activo.	Posibles **Amenazas** sobre cada activo.
		Disponibilidad (1 poca, 5 mucha)	**Integridad** (1 poca, 5 mucha)	**Confidencialidad** (1 poca, 5 mucha)		
Software (BO; JDE; CMA; Correo; Internet; MSOffice; otros)	5	5	5	5	No disponibilidad por caídas de sistema; Falta de integración de sistemas; Fallas de funcionamiento por virus; Falta de conocimientos adecuados para una utilización eficiente. Download de programas no autorizados.	Inutilización por entrada de virus. No accesibilidad por problemas de terceros (ej: CMA)
Hardware (PCs y Notebook)	3	3	3	3	Desprotección / vulnerabilidad; Escasa capacidad de almacenamiento de datos en discos. Obsolescencia por uso y paso del tiempo.	Destrucción por accidentes de personas o fenómenos naturales. Posibilidad de ser robados.
Muebles y útiles (teléfonos fijos y celulares).	2	2	2	2	Obsolescencia por el uso, paso del tiempo o mal uso.	Acceso de personas fuera de la organización; Destrucción por inundaciones, incendios, etc.; Robos o pérdidas
PCs del Centro de Distribución	4	5	3	2	Preservar los activos	Falta de protección
Warehousing (JDE)	5	5	5	5	Errores de sistema	
Indicadores en PC y Servidores	4	5	3	1		
Equipos de radio – frecuencia	5	5	5	3	Red sin seguridad de acceso implementada	Conexiones no autorizadas, robo y malos tratos
Información de S:\DES	5	4	5	5	Integridad; confidencialidad	Hacking; spyware
Información en T:\Formulas	5	5	5	5	Integridad; confidencialidad	Hacking; spyware
Base de datos de Prototipos	5	5	5	5	confidencialidad	Spyware
Base de Seguimiento de proyectos	5	4	5	5	confidencialidad	Spyware
Base de Investigación y desarrollo	4	3	5	5	confidencialidad	Spyware
Base de Especificaciones de productos	4	4	5	4	confidencialidad	Spyware

(continuación...)

1. ¿Hay otros activos que Ud. necesite proteger. (ej.: por leyes o alguna regulación)? Todos los datos de los productos elaborados con trazabilidad a insumos y datos de proceso durante la vida útil de c/u de ellos. La protección de la información en todas sus formas: archivos físicos o electrónicos y el "know-how" de las personas. Información del ISO 9001, se deben guardar por dos años.
2. De los activos que Ud. ha identificado, ¿cuál es el más importante? ¿Por qué? Información de nuevos proyectos; historial de proyectos; información propia en la PC particular. Información (datos); sistemas y software. Sin ellos no podemos trabajar. Información en el servidor (están los registros y estadísticas de la planta en los rubros mencionados de 5 años hasta la actualidad. PCs para la gestión de Mantenimiento y la impresora láser para la impresión de reportes para el mantenimiento preventivo semanal. Las personas, porque por más que se usa software, hay una cantidad de procesos que necesitan conocimientos prácticos. PCs, porque tenemos problemas de disponibilidad del hardware por no poder abrir o guardar correctamente archivos, a veces se guardan "rotos". Especificaciones (sean del Doc9000 o SGDI o del sistema de Especificaciones de productos). Los documentos en archivos PowerPoint, Word, Excel porque contienen información única y en algunos casos confidencial. La información en todas sus formas y archivos. El más importate es Warehousing (JDE) ya que el mismo hace que se realice toda la operación de ingreso y egreso de mercadería. Formulaciones, Prototipos, Seguimiento de Proyectos: son parte de la estrategia de la división y debe ser confidencial.

Hoja de Trabajo - Áreas de preocupación

¿Qué escenarios amenazan sus activos importantes?

Origen de las amenazas

Acciones deliberadas por las personas

Considere:

- ?? ***Personas dentro de la organización (personas ajenas al sector que tienen acceso)***
- ?? ***Personas fuera de la organización (personal de limpieza)***

Acciones accidentales por las personas

Considere:

- ?? ***Personas dentro de la organización***
- ?? *Personas fuera de la organización*
- ?? ***Ud. Mismo (borrar archivos por error)***

Problemas de sistemas

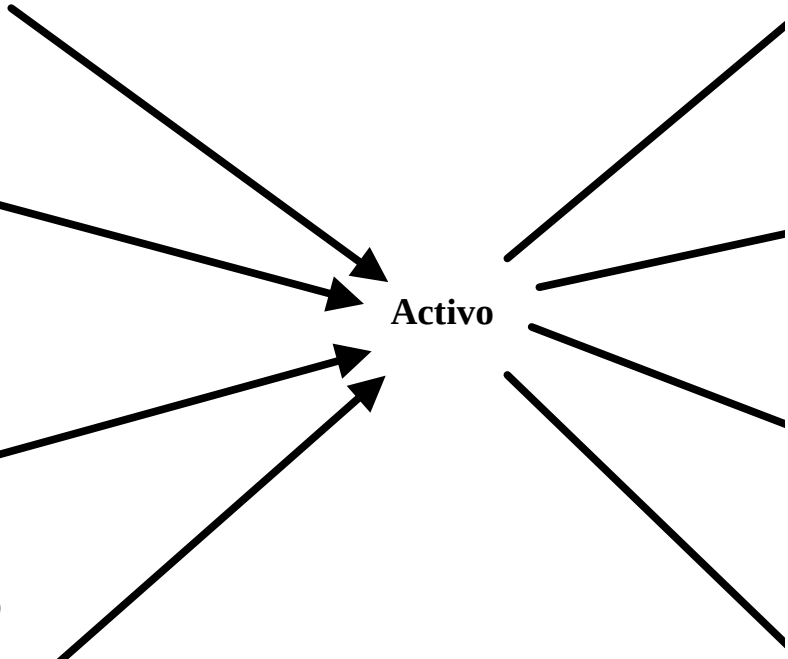
Considere:

- ?? ***Defectos de hardware (obsolescencia)***
- ?? ***Defectos de software***
- ?? ***Indisponibilidad de sistemas relacionados***
- ?? ***Código malicioso (virus, gusanos, Troyanos, back door)***
- ?? *Otros*

Otros Problemas

Considere:

- ?? ***Cortes de energía***
- ?? ***Cortes de las telecomunicaciones***
- ?? *Indisponibilidad del servidor de internet*
- ?? *Inundaciones*
- ?? *Terremotos*
- ?? *otros*



Encuesta a personal clave por sectores

Nombre (opcional): _____

Posición: _____

Encuesta a personal clave	
Practica	**¿Se utiliza esta práctica?**
Conocimiento de la seguridad y entrenamiento	
Las personas entienden la problemática de la seguridad y su responsabilidad.	Sí (**07**) No (**02**) No sabe (**03**)
Hay especialización interna adecuada para todos los servicios, mecanismos, y tecnologías (ej., login, monitoreo, o encriptación), incluyendo su funcionamiento seguro.	Sí (**03**) No (**04**) No sabe (**04**)
Se proveen conocimientos de seguridad, recuerdos periódicos y entrenamiento para todo el personal. Se documenta el avance en conocimientos del personal y se verifica periódicamente.	Sí (**01**) No (**08**) No sabe (**03**)
Estrategia de la Seguridad	
La organización incorpora rutinariamente en sus estrategias de negocio consideraciones sobre seguridad.	Sí (**06**) No (**01**) No sabe (**04**)
Las políticas y estrategias de seguridad tienen en cuenta las estrategias de negocio de la organización y sus metas.	Sí (**05**) No (**02**) No sabe (**04**)
Se documentan estrategias de seguridad, metas y objetivos y se repasan rutinariamente. Se ponen al día, y se comunican a la organización.	Sí (**01**) No (**04**) No sabe (**07**)
Administración de la Seguridad	
La dirección asigna fondos suficientes y recursos para la seguridad de la información.	Sí (**01**) No (**00**) No sabe (**10**)
La organización basa sus prácticas de incorporación y desvinculación de personas sobre aspectos de la seguridad de la información.	Sí (**04**) No (**00**) No sabe (**07**)
La organización administra los riesgos de la seguridad de la información, incluyendo ?? evaluación de riesgos para la seguridad de la información ?? toma acciones para mitigar los riesgos de la seguridad de la información	Sí (**02**) No (**00**) No sabe (**09**)
La dirección recibe reportes de rutina relacionados con la seguridad de la información (ej.:, auditorias, registros, evaluación de riesgos y vulnerabilidades).	Sí (**01**) No (**00**) No sabe (**10**)

Políticas y Regulaciones de Seguridad	
Tiene la organización documentación comprensiva, y políticas que se revisan y actualizan periódicamente.	Sí (**01**) No (**00**) No sabe (**10**)
Hay un proceso documentado para la administración de las políticas de seguridad, incluyendo ?? creación ?? administración (incluyendo revisión y actualización periódicas) ?? comunicación	Sí (**01**) No (**00**) No sabe (**10**)
La organización tiene un proceso documentado para evaluar y asegurarse la competencia con políticas de seguridad de la información, las leyes aplicables, las regulaciones, y los requisitos de seguros.	Sí (**00**) No (**00**) No sabe (**11**)
La organización se esfuerza en mantener actualizadas sus políticas de seguridad.	Sí (**03**) No (**00**) No sabe (**08**)
Administración en colaboración sobre la seguridad	
Tiene la organización políticas y procedimientos para proteger la información cuando se trabaja con otras organizaciones (ej.: terceros, colaboradores, subcontratistas, o empresas colegas), incluyendo ?? protección de la información perteneciente a otras organizaciones ?? entendiendo las políticas y procedimientos de seguridad de las organizaciones externas. ?? finalizando el acceso a la información a todo personal externo que ya no trabaje.	Sí (**05**) No (**01**) No sabe (**04**)
Planes de Contingencia	
Se han realizado análisis de operaciones, aplicaciones y criticidad de los datos.	Sí (**03**) No (**01**) No sabe (**07**)
La organización ha documentado, revisado y testeado ?? la continuidad de las operaciones u operaciones de planes de emergencia ?? plan(es) para recuperación ante desastres ?? plan(es) de contingencia para responder ante emergencias.	Sí (**01**) No (**00**) No sabe (**10**)
Planes y Procedimientos para la Seguridad Física	
Existen planes de seguridad y procedimientos para salvaguardar edificios y áreas restringidas. Están documentados y testeados.	Sí (**05**) No (**01**) No sabe (**05**)
Hay políticas y procedimientos documentados para el control de las visitas.	Sí (**10**) No (**00**) No sabe (**01**)
Hay políticas y procedimientos documentados para el control físico de hardware y software.	Sí (**05**) No (**00**) No sabe (**07**)

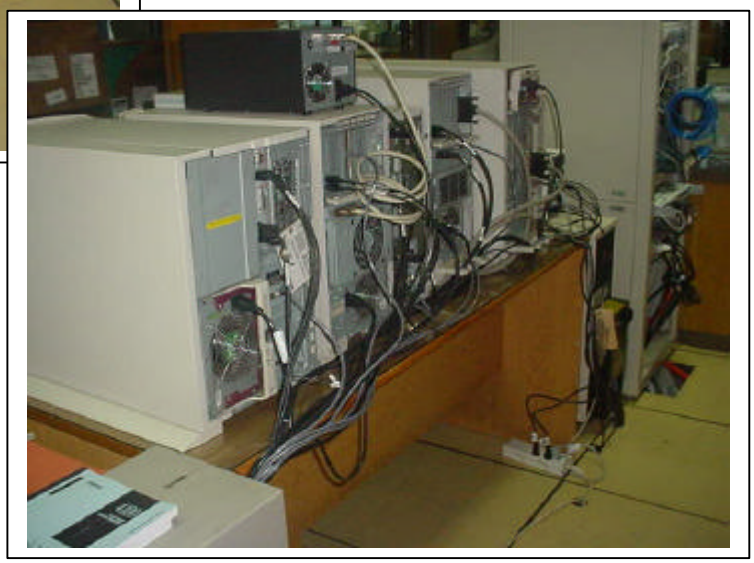
Control del Accesos Físico	
Hay políticas y procedimientos documentados para controlar el accesos físico a las áreas de trabajo, equipamiento (computadores, dispositivos de comunicaciones, etc.) y dispositivos de almacenamiento (software).	Sí (**09**) No (**00**) No sabe (**02**)
Las estaciones de trabajo y otros componentes que tienen accesos a información sensible, tienen controlado el acceso físico para prever accesos no autorizados.	Sí (**06**) No (**03**) No sabe (**01**)
Administración de Sistemas y Redes	
Hay plan(es) documentados y testeados para salvaguardar los sistemas y las redes.	Sí (**06**) No (**00**) No sabe (**06**)
Hay planes de backup documentados y testeados tanto para software como para datos.	Sí (**11**) No (**00**) No sabe (**00**)
El soporte informático entiende sus responsabilidades bajo estos planes de backup.	Sí (**09**) No (**00**) No sabe (**02**)
Autenticación y Autorización	
Hay políticas y procedimientos documentados para otorgar y quitar derechos de acceso a la información para individuos y grupos.	Sí (**08**) No (**00**) No sabe (**03**)
Administración de Incidentes	
Existen procedimientos documentados para identificar, reportar y actuar bajo incidentes sospechosos de seguridad o violaciones.	Sí (**02**) No (**00**) No sabe (**09**)
Los procedimientos de administración de incidentes son periódicamente testeados, verificados y actualizados.	Sí (**03**) No (**00**) No sabe (**08**)
Hay políticas y procedimientos documentados para trabajar con agencias consultoras sobre leyes.	Sí (**01**) No (**00**) No sabe (**11**)
Practicas del Personal en General	
Las personas tienen buenas prácticas de seguridad, como ?? asegurar la información de la cual son responsables ?? no divulgar información sensible a otros (resistencia a la ingeniería social) ?? tener la habilidad adecuada para usar el hardware y el software de tecnología de la información ?? usar buenas prácticas de contraseñas (contraseñas seguras; no las divulgan) ?? entender y seguir políticas y regulaciones de seguridad ?? reconocer y reportar incidentes	 Sí (**10**) No (**00**) No sabe (**02**) Sí (**09**) No (**00**) No sabe (**03**) Sí (**07**) No (**03**) No sabe (**02**) Sí (**07**) No (**04**) No sabe (**02**) Sí (**06**) No (**03**) No sabe (**03**) Sí (**10**) No (**00**) No sabe (**02**)
Hay procedimientos documentados para autorizar y vigilar a todo el personal (incluyendo personal de contratistas) los cuales trabajan con información sensible o en lugares donde se encuentra la información.	Sí (**02**) No (**01**) No sabe (**09**)

Estrategia de protección
1. ¿Qué aspectos de esta encuesta consideraría discutir con más detalle? Políticas de seguridad y procedimientos al respecto. Todo lo que no sabemos relacionado con Seguridad Informática. Cómo hacer más segura la información confidencial.
2. ¿Qué asuntos importantes no están cubiertos por esta encuesta? La capacitación relacionada con Seguridad Informática. Uniformidad corporativa en seguridad informática. Comunicación de estrategias de seguridad informática y capacitación. Cuáles son los procedimientos para el intercambio de PC's de una persona a otra. Como se mantienen los datos y cómo se borran (los "favoritos" inclusive)
3. ¿Hay políticas de seguridad específicas, procedimientos o prácticas aunque sea para algunos de los elementos mencionados? ¿Cuáles? Existen prácticas de backup contenido en los distintos software. Existen usuarios con perfiles de habilitación (Spac, JDE, Doc9000, Lotus). Es práctica habitual el cambio de clave. Sí. Claves de accesos para cada perfil; y accesos remoto a la red. Hay procedimientos de backup. El resto "no sé".
4. ¿La estrategia de protección de la compañía es efectiva? No puedo saberlo. ¿Por qué motivos?: Mis conocimientos en informática no son tan extensos como para conocer esto. Se necesita más análisis. Sí. ¿Por qué motivos?: Porque hasta el momento no han existido fugas de información importantes. No sabemos. ¿Por qué motivos?: Desconocemos si ha habido fuga de información. No. ¿Por qué motivos?: No hay una estrategia que contemple todas las alternativas y todas las personas y de lo que hay no existe divulgación. Parcialmente efectiva. ¿Por qué motivos?: a)falta de comunicación y capacitación; b)falta de actitud en general para aplicar políticas de seguridad; c)presencia de algunos eventos en donde se probaron las políticas de seguridad. No la conozco. A nivel correo electrónico es más efectiva que hace unos años. En otros niveles no conozco casos.

Anexo 4 (Registros gráficos del centro de cómputos.)

A continuación se detallan los cambios realizados en las oficinas del centro de cómputos en vistas de mejorar la seguridad de acceso a la sala y de reducción de riesgos físicos.

ANTES de aplicar los controles de seguridad mencionados en el apartado correspondiente:



DESPUÉS de aplicar los controles de seguridad física:

Anexo 5 (Requisitos de RRHH para el acceso de proveedores)

Arcor SAIC
División Chocolates
Planta Colonia Caroya

SRES. CONTRATISTAS:

REQUISITOS PARA INGRESO E M P R E S A S

SEÑORES CONTRATISTAS : PARA PODER INGRESAR A PRESTAR SERVICIOS EN NUESTRA PLANTA DEBERÁN ENTREGAN ANTES DE LA PRESTACIÓN LA SIGUIENTE DOCUMENTACIÓN :

FOTOCOPIA DE LOS RECIBOS DE HABERES DEL MES INMEDIATO ANTERIOR DE LOS EMPLEADOS QUE TRABAJEN EN NUESTRA PLANTA (DEBE ESTAR LA FIRMA DEL TRABAJADOR Y EL CORRESPONDIENTE NÚMERO DE C.U.I.L) EN CASO DE TRABAJADORES NUEVOS, DEBERÁN ADJUNTAR CLAVE DE ALTA TEMPRANA
FOTOCOPIA FIRMADA POR EL TITULAR DE LA EMPRESA CONTRATISTA DE LA CONSTANCIA DE PAGOS MENSUALES AL SISTEMA DE SEGURIDAD SOCIAL. (DECLARACIÓN JURADA Y CONSTANCIA DE PAGO)
FOTOCOPIA FIRMADA POR EL TITULAR DE LA EMPRESA CONTRATISTA DE LAS DIFERENTES PAGINAS QUE INTEGRAN LA IMPRESIÓN DEL FORMULARIO 931 O SIMILAR.
LISTADO DE PERSONAL QUE INGRESARA A NUESTRA PLANTA Y POR EL TRANSCURSO APROX. DE TIEMPO QUE DURARA LA PRESTACIÓN SUSCRIPTA POR EL TITULAR O REPRESENTANTE LEGAL DE LA EMPRESA
CONSTANCIA DE PAGO ART, CON LISTADO INFORMADO POR DICHA ENTIDAD, QUE CERTIFIQUE QUE EL PERSONAL QUE SÉ DESEMPEÑA EN NUESTRA EMPRESA ESTÁ CUBIERTO POR LA ASEGURADORA DE RIESGOS DEL TRABAJO. DEBE INCLUIRSE EN LA CONSTANCIA DE AFILIACIÓN EL SIGUIENTE TEXTO O SIMILAR: "ESTA ASEGURADORA RENUNCIA A EJERCER CONTRA ARCOR Y/O SUS SOCIEDADES CONTROLADAS O ACCIONARIAMENTE VINCULADAS QUE ESTA ASEGURADORA DECLARA CONOCER, LOS DERECHOS DEL ARTICULO 39 INC. 5 DE LA LEY 24.557(LEY DE RIESGOS DE TRABAJO)" ESTA COPIA TAMBIÉN DEBE ESTAR FIRMA POR EL TITULAR DE LA EMPRESA CONTRATISTA.
NOTIFICACIÓN BANCARIA DONDE CONSTE QUE LA EMPRESA CONTRATISTA ES TITULAR DE UNA CUENTA CORRIENTE BANCARIA. (POR ÚNICA VEZ)

DICHA DOCUMENTACIÓN CONSTITUYE UNA CONDICIÓN INDISPENSABLE PARA PODER REALIZAR CUALQUIER TIPO DE SERVICIO Y/O CONTRATACIÓN CON NUESTRA EMPRESA . EN CASO DE CONTINUAR LA PRESTACIÓN , ESTA DOCUMENTACIÓN SERÁ RENOVADA CADA MENSUALMENTE, DEBIENDO EFECTUAR LA ENTREGA ANTES DEL DIA 15 DE CADA MES.-

DE NO CUMPLIR CON LA ENTREGA DE LA DOCUMENTACIÓN ANTES DEL INICIO DE LA PRESTACIÓN, LA MISMA SE POSTERGARA HASTA QUE CUMPLAN CON LO REQUERIDO.

ATTE

FIRMA Y ACLARACIÓN RESPONSABLE EMPRESA CONTRATISTA: .....

FECHA : / / .-

Anexo 6 (Requisitos de MAHPI para el acceso de proveedores)

ARCOR S.A.I.C.
División Chocolates
Planta Colonia Caroya

At CONTRATISTAS

De nuestra mayor consideración:

Para autorizar el ingreso de Empresas contratistas a realizar obras, tareas o trabajos adjudicados y que deban llevarse a cabo en el interior del predio fabril de ARCOR S.A.I.C. División Chocolates, Planta Colonia Caroya, deberán cumplimentar con los requisitos de Seguridad que se detallan más abajo:

1. Memoria Técnica y Programa de Seguridad de la obra o tareas (según Res. 51/97) y hacerla extensiva a toda obra que implique riesgo y que no sea de la actividad de construcción

   Con los siguientes ítems:
   # Riesgos de la tarea.
   # Medidas de control.
   # Capacitación recibida y a recibir por el personal (adjuntar certificados)
   # Elementos de protección personal entregado y a entregar al personal (adjuntar constancia de recepción).

   Esta información deberá estar firmada por:
   # El empleador.
   # Responsable de Higiene y Seguridad en el Trabajo de la Empresa Contratista.

   Aprobada todo por la ART que ampara los riesgos del trabajo de la Empresa Contratista.

2. Visita a obra del responsable de Higiene y Seguridad con la carga horaria de acuerdo a lo establecido por la Res. 1338.
3. Constancia de visita del Responsable de Higiene y Seguridad del Contratista y recomendaciones brindadas al personal y asimismo donde también se dejara escritas las observaciones realizadas en obra. En todos los casos esta constancia debe quedar copia en la Oficina de Mahpi.
4. Listado de los Servicios Asistenciales de la Zona que brindarán atención médica al personal en caso de accidente de trabajo (Nombre, Dirección y Teléfono).
5. El personal a ingresar deberá contar en todo momento con los Elementos de Seguridad requeridos para las tareas que realicen.
6. Las máquinas y equipos deberán estar en buenas condiciones y con todas las protecciones necesarias, eléctricas como mecánicas. Las mismas serán verificadas por Mahpi antes de su ingreso a planta y durante el desarrollo de las actividades en las auditorias.
7. Las empresas contratistas que realicen trabajos de soldadura deberán contar con un matafuego de polvo químico de 5 Kg., mínimo, por equipo de soldadura a utilizar.

Sin otro particular, saludamos a Ud. Atte.-

Anexo 7 (compromiso de confidencialidad)

Reconocimiento de propiedad y compromiso de confidencialidad en el manejo y conocimiento de información.

?? En razón de los servicios de ....., que a través de mis propios medios técnicos y humanos brindo a ARCOR S.A.I.C. y/o sus empresas vinculadas y/o relacionadas, declaro que cualquier invención, descubrimiento o desarrollo del que yo o el personal que de mí dependa resulte autor –exclusivo o no- en ocasión y por el hecho de la prestación de tales servicios, será considerado de propiedad de ARCOR S.A.I.C. y/o sus empresas vinculadas y/o relacionadas.

?? Me comprometo asimismo, respecto de tales invenciones, descubrimientos o desarrollos, como asimismo respecto de cualquier otro método, fórmula, diseño, material, proceso, desarrollo, combinaciones y en general, de toda otra información a la que yo y mis dependientes podamos acceder en ocasión y por el hecho de los servicios que presto para ARCOR S.A.I.C. y/o sus empresas vinculadas y/o relacionadas, a guardar y hacer que mis dependientes guarden, estricta reserva, y a no divulgarlos ni utilizarlos –ni permitir se sean divulgados ni utilizados por mis dependientes- fuera del ámbito de la referida empresa, ya fuera durante el desempeño de los servicios que brindo a la misma, o luego de finalizados éstos.

?? Será considerada violación de esta obligación, el mero retiro de la empresa, cualesquiera sean sus fines, de materiales, bibliografía, información en general, sin que medie expreso consentimiento de parte de ARCOR S.A.I.C. y/o sus empresas vinculadas y/o relacionadas.

?? Quedo debidamente notificado, en función de lo expuesto, que la violación de mi parte o de las personas que de mí dependan, del secreto y reserva a que me comprometo precedentemente, será considerado grave incumplimiento de las obligaciones contractuales a mi cargo, y autorizará a ARCOR S.A.I.C. y/o sus empresas vinculadas y/o relacionadas a rescindir con justa causa el contrato de locación de servicios que nos vincula, y a reclamar los daños y perjuicios que tal incumplimiento le ocasione, sin perjuicio de la aplicación de otras sanciones legales que en derecho correspondan.

Suscribo el presente, a los.....días del mes de..... de.....

Firma: .....

Aclaración: .....

Glosario y siglas.

Términos informáticos:

_a_____

Access Point (AP): Dispositivo inalámbrico central de una WLAN que mediante sistema de radio frecuencia (RF) se encarga de recibir información de diferentes estaciones móviles bien para su centralización, bien para su enrutamiento.

Administrador: Persona que se encarga de todas las tareas de mantenimiento de un sistema informático. Tiene acceso total y sin restricciones al mismo. Véase También Root y SysOp.

ANSI (American National Standard Institute): Asociación sin fines de lucros, formada por fabricantes, usuarios, compañías que ofrecen servicios públicos de comunicaciones y otras organizaciones interesadas en temas de comunicación. Es el representante estadounidense en **IS**O. Que adopta con frecuencia los estándares ANSI como estándares internacionales.

Antivirus: Programa que encargado de evitar que cualquier tipo de virus ingrese al sistema, se ejecute y se reproduzca.. Para realizar esta labor existen muchos programas, que comprueban los archivos para encontrar el código de virus en su interior.

Archivo: Conjunto bytes relacionados y tratados como una unidad. Un archivo puede contener programas, datos o ambas cosas.

ARP (Address Resolution Protocol): Este Protocolo de Resolución de Direcciones permite mantener asignaciones de pares formados por las direcciones **IP** y las direcciones físicas **(MA**C) de los distintos dispositivos de comunicación.

AS/400 - OS/400: Serie de grandes ordenadores creados por IBM **Os/400 es un** Sistema operativo multitarea y multiusuario creado por IBM para sus sistemas AS/400.

ASCII (American Standard Code for Information Interchange): Código estándar americano para intercambio de información. Sistema de codificación de 7 **bits** que asigna un número del 0 al 127 a cada letra, número, caracteres especiales y de control recogidos. El uso del octavo bit no está tan estandarizado aunque se suele utilizar como código de paridad calculado (normalmente par).

_b_____

Backdoor: Puerta trasera de entrada a una computadora, programa o sistema en general. Es utilizado para acceder sin usar un procedimiento normal.

Backup: Copia de seguridad que se realiza con el fin de mantener los datos en forma segura.

Bastión Host: Sistema configurado para resistir los ataques y que se encuentran instalado en una red en la que se prevé que habrá ataques. Son componentes de los Firewalls ejecutando alguna aplicación o sistema operativo de propósito general.

BIOS (Basic Input Output System): Sistema básico de entradas y salidas. Microprogramación que reside permanentemente en los microordenadores y que controla las operaciones de entrada y salida.

Bit: En informática, unidad mínima de información.

Bomba Lógica: Programa ilegítimo contenido dentro de un sistema y que ante un hecho o una fecha prevista "explota" causando daño al sistema que lo contiene u a otro.

BPS (Bits por Segundo): Medida de velocidad de transmisión.

BroadCast: Difusió**n.** Tipo de comunicación en que todo posible receptor es alcanzado por una sola transmisión.

Browser: Software empleado para aprovechar diversos recursos de Internet. Es comúnmente llamado **Navegador.**

Buffer Overflow: Error generado cuando un programa recibe una entrada mayor a la que espera, sobrescribiendo áreas críticas de memoria.

Bug: Un error en un programa o en un equipo. Se habla de bug si es un error de diseño, no cuando la falla es provocada por otro motivo.

Byte: Combinación de **Bit**s. En la representación más común 8 bits forman un byte.

_C_____

Caballo de Troya: Programa aparentemente útil el cual contiene código adicional escondido, desarrollado para obtener algún tipo de información o causar algún daño.

Carpeta: Unidad de agrupamiento que tienen los sistemas para mostrar la información a los usuarios para ser accedida más fácilmente.

Cifrar: Ver **Criptografí**a.

Clave Privada: En un **Sistema Asimétrico de Cifrado** es la clave que solo el emisor del mensaje conocen para **cifrar** o descifrar un mensaje.

Clave Pública: En un **Sistema Asimétrico de Cifrado** es la clave que todos conocen para **Cifrar** o descifrar un mensaje.

Clave, Contraseña (Password): palabra o frase que permite acceder a un sistema, encriptar un dato, determinar privilegios de usuarios, etc.

Cliente: Sistema o proceso que solicita a otro sistema o proceso que le preste un servicio. Una computadora que solicita el contenido de un archivo a otra **(Servidor)** es un cliente de la misma.

Código Fuente: Un programa escrito en un formato entendible por el hombre pero no por la computadora. Necesita ser "traducido" a código máquina para ser interpretado por esta última.

Código malicioso (Malware): Es un término genérico utilizado para describir el software malicioso tales como: virus, troyanos, etc.

Contingencia: Situación que genera la imposibilidad de cumplir las tareas habituales mediante la operatoria habitual.

Correo electrónico: Aplicación que permite enviar mensajes a otros usuarios de la red sobre la que esté instalado. También denominado **E-Mai**l.

Cracker: Persona que quita la protección a programas con sistemas anticopia. Hacker maligno, que se dedica a destruir información.

Criptografía: Ciencia que consiste en transformar un mensaje inteligible en otro que no lo es, mediante la utilización de **clave**s, que solo el emisor y receptor conocen.

Criticidad: Propiedades de la información que la describe de mayor o menor riesgo para los objetivos de negocio de la compañía.

Cuentas de Usuarios: Conjunto de caracteres que identifica a cada uno de los usuarios en el proceso de acceso a los sistemas.

_d_____

Denial of Service (DoS): Negación de Servicio. Acciones que impiden a cualquier sistema funcionar de acuerdo con su propósito.

Detección de Intrusos: Sistemas que agrupa un conjunto de técnicas cuyo propósito es detectar las intrusiones en una computadora o un sistema.

Diccionarios: Conjunto de palabras almacenadas en un archivo. Su fin es utilizar cada palabra para ser probada como posible **Password** de un sistema que se quiere violar. Véase también **Fuerza Bruta.**

DMZ: Ver **Zona Desmilitarizada**

DNS (Domain Name Server): Servicio que proporciona una dirección IP a partir de un nombre de dominio proporcionado. Este protocolo evita tener que recordar las complicadas combinaciones de números que forman una dirección IP.

_e_____

E-Mail: Ver **Correo Electrónic**o.

Emergencia: Circunstancia no esperada en la operación de los sistemas o en los procesos de utilización de la información contenida en dichos sistemas.

Equipos: Recursos informáticos físicos para el procesamiento, transmisión y/o conservación de datos.

Ethernet: Protocolo de comunicación. Especificación de LAN de banda base, inventada por Xerox Corporation y desarrollada conjuntamente por Xerox, Intel, y Digital Equipment Corporation.

Exploit: Programa que aprovecha un **Bug** de un sistema. Programa que abusa de algún error de un sistema operativo para conseguir aumentar los privilegios de un usuario o la caída del sistema.

f

Firewall: Barrera de protección. Es un procedimiento de seguridad que coloca un sistema de computación programado especialmente entre una red segura y una red insegura. Un sistema o combinación de sistemas que fija los límites entre dos o más redes y restringe la entrada y salida de la información.

FTP (File Transfer Protolol): Protocolo del nivel de usuario (protocolos de aplicación) para la transferencia de archivos entre computadoras. También pueden hacer referencia a la aplicación que permite transferir archivos de una computadora a otra usando el mismo protocolo.

Fuerza Bruta: Se basan en aprovechar **Diccionarios** para comparar las palabras almacenadas en él con las **Passwords** del sistema y obtenerlos.

g

Gateway: Dispositivo de enrutamiento. En la actualidad, se utiliza el término **Router** para describir los nodos que realizan esta función, mientras que **Gateway** se refiere a un dispositivo para fines especiales que convierte información de la capa de aplicación de un stack de protocolo a otro.

Guest (Invitado): Cuenta pública en un sistema. Su objetivo es ser utilizada por alguien que no tiene una cuenta propia.

Gusano: Programa ilegítimo que es capaz de reproducirse a si mismo infinitas veces hasta colapsar el sistema, en el que se está ejecutando, por falta de recursos.

h

Hacker: Una persona que disfruta explorando los detalles de las computadoras y de cómo extender sus capacidades.

Handshake (Saludo): Secuencia de mensajes intercambiados entre dos o más dispositivos de red para garantizar la sincronización de la transmisión.

Hardware: Componentes electrónicos, tarjetas, periféricos y equipo que conforman un sistema de computación.

Hexadecimal: Base 16. Una representación numérica que utiliza los dígitos 0 a 9, con su significado usual, más las letras A a F para representación de los dígitos hexadecimales con valores de 10 a 15.

Host: Sistema Central. Computadora que permite a los usuarios comunicarse con otros sistemas de una red. Los usuarios se comunican utilizando programas de aplicación, tales como el **Correo Electrónic**o, **Telnet** y **FT**P.

HTML (HyperText Markup Language): Formato especial de archivos sobre el que está basada la estructura de la aplicación **WWW (World Wide Web**).

HTTP (HyperText Tranfer Protocol): Es un protocolo de la capa de aplicaciones con la velocidad necesaria para sistemas de información hipermediales en un ambiente distribuido y colaborativo.

Hub (Concentrador): Dispositivo que sirve como centro de una red de topología en estrella.

I

ICMP (Internet Control Message Protocol): Protocolo utilizado para gestionar la comunicación de mensajes de error entre distintos puntos de la red.

ID: Identificación.

IDEA (International Data Encription Algorithm): Algoritmo de encriptación simétrico.

IEEE (Institute of Electrical and Electronics Engineers): Instituto de ingeniería eléctrica y electrónica. Organización profesional entre cuyas actividades se incluye el desarrollo de estándares para comunicaciones y **Rede**s.

Ingeniería Social: Arte de convencer a la gente para que realice actos que pueden comprometer un sistema. Obtención de información por medios ajenos a la informática.

Internet: Sistema de redes de computación ligadas entre si, con alcance mundial, que facilita servicios de comunicación de datos como registro remoto, transferencia de archivos, correo electrónico y grupos de noticias.

Intruso: Aquella persona que con una variedad de acciones intenta comprometer un recurso de hardware o software.

Invitado: Ver **Guest.**

IP (Internet Protocol): Protocolo de comunicación sin conexión, que por sí mismo proporciona un servicio de datagramas. Es el Protocolo que proporciona el servicio de envío de paquetes para los protocolos soportados **TC**P, **UDP** e **ICM**P. Protocolo de capa de red de la pila **TCP/IP** que ofrece un servicio de internetwork sin conexión. El IP tiene prestaciones para direccionamiento, especificación del tipo de servicio, fragmentación y rearmado, y seguridad.

IP Spoofing; Método para falsear la **IP** en una conexión remota.

IPSec: Protocolo creado por el IETF para brindar seguridad a nivel de red.

IPX/SPX: Es el conjunto de protocolos de bajo nivel utilizados por el sistema operativo de red Netware de Novell. SPX actúa sobre IPX para asegurar la entrega de los datos.

ISO (International Organization for Standarization): Organización voluntaria, no gubernamental, cuyos miembros han desarrollado estándares para las naciones participantes. Uno de sus comités se ocupa de los sistemas de información. Han desarrollado el modelo de referencia **OSI** y protocolos estándares para varios niveles de este modelo.

ITSEC: Criterios Comunes de Evaluación de la Seguridad de los Productos y Sistemas de Información.

_k_

Kerberos: Sistema de seguridad en el que los login y los passwords viajan encriptados a través de la red.

Key Logger: Grabador de teclas pulsadas. Es utilizado cuando se desea conocer las contraseñas, nombres de usuarios o cualquier otra información en donde se utilice el teclado como vía de entrada al sistema.

_l_

L2TP (Layer To Tunneling Protocol): protocolo estándar que encapsula las tramas que van a enviarse a través de redes.

LAN (Local Area Network): Red de área local. Red de datos de alta velocidad y bajo nivel de error que cubre un área geográfica relativamente pequeña (hasta unos pocos miles de metros). Las LANs conectan estaciones de trabajo, periféricos, terminales y otros dispositivos en un único edificio u otra área geográficamente limitada. Véase también **MAN** y **WA**N.

Linux: Sistema Operativo de la familia **UNI**X.

Log: Archivo de registro de actividades.

Login: Nombre de acceso de un usuario a una red o sistema multiusuario. Este término se le puede aplicar tanto al nombre de su cuenta como al hecho de ingresar a un sistema de este tipo. El usuario debe usar el nombre, así como su contraseña (password), para tener acceso al sistema.

_m_

MAC (Media Access Control): Control de acceso al medio. La inferior de las dos subcapas de la capa de enlace de datos definida por **IEE**E. La subcapa **MAC** administra el acceso a medios compartidos.

Mac Address (Media Access Control Address): Dirección hardware de 6 bytes (48 bits) única que identifica únicamente cada nodo (tarjeta) de una red y se representa en notación hexademinal. En redes IEEE 802, la capa Data Link Control (DLC) del Modelo de Referencia OSI se divide en dos sub-capas: Logical Link Control (LLC) y Media Access Control (MAC), la cual se conecta directamente con el medio de red. Consecuentemente, cada tipo de medio de red diferente requiere una capa MAC diferente. En redes que no siguen los estándares IEEE 802 pero sí el modelo OSI , la dirección del nodo se denomina Data Link control (DLC) address.

MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

MainFrame: Gran computadora central.

MAN (Metropolitan Area Network): Red de área metropolitana. En general, una MAN abarca un área geográfica más vasta que una **LA**N, pero cubre un área geográfica más pequeña que una **WA**N.

Módem (Modulador-Desmodulador): Conexión del equipo del usuario final que permite transmitir datos digitales a través de dispositivos de transmisión analógicos, como las líneas telefónicas.

_n_____

Negación de Servicio: Ver **DoS.**

Network (Red): Red de computadoras es un sistema de comunicación de datos. Conecta entre sí sistemas informáticos situados en diferentes lugares. Puede estar compuesta por diferentes combinaciones de diversos tipos de redes.

Network spoofing: Técnica basada en la creación de tramas TCP/IP utilizando una dirección IP falseada; desde su equipo, un atacante simula la identidad de otra máquina de la red (que previamente ha obtenido por diversos métodos

Nodo: Cualquier computadora o periférico conectado directamente a una red.

Notebook: Computadora portátil (laptop) de tamaño y peso reducidos.

NTFS (New Technology File System): Sistema de archivos diseñado específicamente para Windows NT**.**

Número IP: Número que identifica de manera única una maquina dentro de la red que utiliza el **Protocolo TC**P.

_o_____

OCTAVE^{SM} (Operationally Critical Threat, Asset, and Vulnerability Evaluation^{SM}): **Método** de Implementación de estrategias de seguridad informática; Carnegie Mellon.

OSI: Open System Interconnection): Interconexión de sistemas abiertos. Programa de estandarización internacional creado por **ISO** e **ITU-T** para desarrollar normas para networking de datos que faciliten la interoperabilidad entre equipos de diversos fabricantes.

_p_____

Password (Clave): Ver **Clav**e, **Contraseñ**a.

Patch (Parche): Modificación de un programa ejecutable para solucionar un problema, corregir un **Bug** o para cambiar su comportamiento.

PC (Personal Computer): Computadora Personal.

Perfil de Usuario: Información a la que el usuario necesita acceder para el desarrollo de sus tareas, criticidad de la información, funciones del puesto, etc.

Personal: Todo el personal de la compañía y los terceros que interactúan de manera habitual u ocasional

PGP (Pretty Good Privacy): Privacidad Bastante Buena. Programa de encriptación de correo electrónico para Internet, que utiliza una combinación de claves públicas y privadas.

Pirata Informático: Persona que copia software, con derecho de autor, ilegalmente sin que medie el permiso expreso del desarrollador. No confundir con el término **Hacker** o **Cracke**r.

PLC (Programmable Logic Controllers): Sistema autómata programable para aplicaciones de automatización industrial.

PPTP (Point to Point Tunneling Protocol): Protocolo antecesor de **L2TP** fue diseñado para proporcionar comunicaciones autenticadas y cifradas entre un cliente y un **Gateway** o entre dos Gateways.

Promiscuo (Modo): Normalmente interfaz **Ethernet** que permite leer toda la información sin importar su destino, aplicable a un segmento de **Re**d.

Protocolo: Conjunto de normas (lenguaje de reglas y símbolos) que rige cada tipo de comunicación entre dos computadoras (intercambio de información).

Proxy: Entidad que, a fin de lograr mayor eficiencia, esencialmente suple otra entidad.

Puerto: Proceso de capa superior que está recibiendo información de capas más bajas.

_r_____

RAID (Redundant Array Of Independent Disks): es un término inglés que hace referencia a un conjunto de discos redundantes independientes. Este tipo de dispositivos se utilizan para aumentar la integridad de los datos en los discos, mejorar la tolerancia a los fallos y errores y mejorar el rendimiento.

RAS (**Remote Access Server):** Servidor dedicado a la gestión de usuarios que no están en una red pero necesitan acceder remotamente a ésta. Permite a los usuarios, una vez autenticados, obtener acceso a los archivos y servicios de impresora de una LAN desde una localización remota.

Recursos informáticos: Conjunto de elementos de hardware y software que conforman un sistema.

Red: Conjunto de computadoras, impresoras, **Router**s, **Switche**s, y otros dispositivos, que pueden comunicarse entre sí por algún medio de transmisión.

Root: Persona que se encarga del mantenimiento del sistema. Tiene acceso total y sin restricciones al mismo. Véase también **Administrador** y **SysO**p.

Router: Dispositivo que distribuye tráfico entre redes. La decisión sobre a dónde enviar se realiza en base a información de nivel de red y tablas de direccionamiento. Ver también: **Gateway.**

_S_____

SANS The SANS Institute

SCADA (System Control And Data Acquisition): Sistemas de Control y Adquisición de Datos

Server (Servidor): Máquina que ofrece servicios a otras dentro de una red. También llamado **Host.**

Servicios: Software particular que se utiliza para la ejecución de ciertas funciones del área de Sistemas

SSID - RFID – ESSID (Radio Frequency Identification): identificador de red inalámbrica, similar al nombre de la red pero a nivel WI-FI.

SI: Seguridad Informática.

Sistema Asimétrico de Cifrado: Sistema mediante el cual se emplea una doble **Clave** kp **(privad**a) y KP **(Públic**a). Una de ellas es utilizada para **Cifrar** y la otra para descifrar. El emisor conoce una y el receptor la otra. Cada clave no puede obtenerse a partir de la otra.

Sistema Simétrico de Cifrado: Sistema mediante el cual se emplea la misma **Clave** para **Cifrar** y descifrar. El emisor y receptor deben conocerlas.

SMTP (Simple Mail Transfer Protocol): Protocolo que proporciona la capacidad de almacenamiento y reenvío del correo entre los host de los sistemas de correo de la red.

Sniffer: Es un programa que permite "escuchar furtivamente" en redes de medios de comunicación compartidos (tales como **Etherne**t). Se ejecuta en una máquina que está conectada a la red, en modo **Promiscuo** y captura el tráfico de todo el segmento de red.

SNMP (Simple Network Management Protocol): Protocolo que permite obtener información de gestión de los dispositivos conectados a la red.

Socks: Protocolo que permite la conexión a equipos situados detrás un **Firewal**l.

Software: Programas de sistema, utilerías o aplicaciones expresadas en un lenguaje de maquina.

SPAC: Sistema para el aseguramiento de la calidad; http://www.druida.com.ar/ - abril de 2004

Spam: También conocido como *junk-mail o correo basura*, consiste en la práctica de enviar indiscriminadamente mensajes de correo electrónico no solicitados que, si bien en muchos casos tienen meramente un fin publicitario, lo que pueden provocar es un aumento de ancho de banda en la red.

Spyware: Pequeñas aplicaciones cuyo fin es el de obtener información, sin que el usuario se de cuenta, de tipo comercial. Generalmente se encuentran dentro de aplicaciones gratuitas en Internet.

SSL (Secure Sockets Layers): Protocolo que provee una conexión segura entre dos hosts.

SUN OS: Sistema Operativo de la empresa Sun. Es una implementación de **Uni**x.

Switch: Dispositivo que opera en la capa de enlace de datos del modelo **OSI**. Dispositivo electrónico o mecánico que permite establecer una conexión cuando resulte necesario y terminarla cuando ya no hay sesión alguna que soportar.

SysOp: Persona que se encarga del mantenimiento del sistema. Tiene acceso total y sin restricciones al mismo. Véase también **Administrador** y **Roo**t.

_t_____

TCP (Transmission Control Protocol): Este Protocolo de Control de Transmisión es un protocolo orientado a conexión. Su función principal es proporcionar mecanismos que ofrezcan seguridad en el proceso de entrega de los paquetes a su destino, así como ordenar paquetes de información y evitar la repetición de éstos.

TCP/IP (Tranfer Control Protocol/Internet Protocol): Arquitectura de red con un conjunto de protocolos que permiten compartir recursos a través de una red. Este familia de protocolos es la más importante difundido en la actualidad, por ser la base de **Internet**.

TI (Information Technology): Tecnología Informática o Tecnología de la Información.

Trashing: Arte de revolver la basura para encontrar información útil.

Troyano: Programa legítimo que ha sido alterado de alguna forma y que contiene funciones desconocidas (generalmente dañinas). Véase también **Caballo de Troya.**

_u_

UNIX: Sistema operativo utilizado por la gran mayoría de máquinas de Internet.

UPS (Uninterrupted Power Suply): Sistema de energía ininterrumpido.

Username (Usuario): Nombre único que identifica a un usuario, y es utilizado como medio de identificación ante un sistema.

_v_

Virus: Programa de actuar subrepticio para el usuario; cuyo código incluye información suficiente y necesaria para que, utilizando los mecanismos de ejecución que le ofrecen otros programas, puedan reproducirse y ser susceptibles de mutar; resultando de dicho proceso la modificación, alteración y/o daño de los programas, información y/o hardware afectados.

VPN (Virtual Private Network): Red Privada Virtual, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

Vulnerabilidad: Hardware, firmware o **Software** que contiene **Bugs** que permiten su explotación potencial.

_w_

WAN (Wide Area Network): Red de área extensa. Red de comunicación de datos que sirve a usuarios ubicados a través de una amplia zona geográfica y a menudo utiliza dispositivos de transmisión suministrados por portadoras comunes. Véase también **LAN** y **MA**N.

Web Sites (Sitio Web): Sistema dedicado al intercambio de información **On-Lin**e.

Windows: Sistema Operativo gráfico de la empresa Microsoft.

Worm: Ver **Gusan**o.

WWW (World Wide Web): Gran red de servidores de Internet que brinda servicios de hipertexto y otros a las terminales que corren aplicaciones cliente como por ejemplo un explorador WWW.

Z

Zona Desmilitarizada (DMZ): Segmento físico de la red que tiene conexión con la red de Internet.

Otros Términos:

AFIP: Administración Federal de Ingresos Públicos.

ART: Aseguradora de Riesgos de Trabajo.

CONCA: equipo clave del proceso donde tiene lugar el mayor trabajo mecánico, homogeneización, pérdida de volátiles y disminución de contenido de agua.

HACCP: Hazard Analysis Critical Control Point - Análisis de Riesgos y Puntos Críticos de Control. Sistema de prevención para eliminar o minimizar potenciales riesgos físicos, biológicos o químicos para la seguridad y calidad de productos alimenticios.

MAHPI: Área de Medio Ambiente, Higiene y Protección Industrial.

SGI: Sistema de Gestión Integral (sigla utilizada en ARCOR).

TPM: (Total Productive Maintenance), Mantenimiento Productivo Total; El TPM es un sistema desarrollado en Japón, para eliminar pérdidas, reducir paradas, garantizar la calidad y disminuir costes en las empresas con procesos continuos.

VRC y PDT: La empresa **Symbol** llama así a algunos de sus modelos de unidades móviles de equipos de radio frecuencia, **VRC:** Vehicle Radio Computer y **PDT:** Portable Data Terminal.

Bibliografía.

- MICROSOFT; "Guía de operaciones de seguridad para Windows 2000 Server; Capítulo 4: Asegurar servidores basándose en su función"; http://www.microsoft.com/spain/technet/seguridad/2000server/chapters/ch04secops.aspx - abril de 2005.
- ALDEGANI, Gustavo. Miguel. Seguridad Informática. MP Ediciones. 1° Edición. Argentina. 1997. Página 26.
- CALVO, Rafael Fernández. "Glosario Básico Inglés-Español para usuarios de Internet", 1994-2001: http://www.ati.es/novatica/glointv2.thml - abril de 2004, rfcalvo@ati.es
- CANO, Jeimy J.; "Pautas y Recomendaciones para elaborar Políticas de Seguridad Informática"; http://derechotecnologico.com/estrado/estrado004.html - marzo de 2005.
- GRATTO, Pierre; Protección Informática, Ed. Trillas, México, 1998
- HERZOG Pete; Manual de la Metodología Abierta de Testeo de Seguridad OSSTMM 2.1- 23 de agosto de 2003; ISECOM (Institute For SECurity And Open Methodologies)
- MACCARE DESARROLLOS; "Glosarios"; http://www.maccare.com.ar/glosario.htm - mayo de 2005.
- MAGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.
- Manual de Seguridad de ArCERT: Coordinación de Emergencia en Redes Teleinformáticas.
- MARTIN-GULLAN PRODUCTIONS; "Glosario de términos informaticos Inglés-Español" http://www.geocities.com/Athens/2693/glosario.html - mayo de 2005.
- Norma IRAM 17799, Traducción de la norma ISO/IEC 17799:2000 "La gestión de la seguridad" Estándar para la gestión de la seguridad de la información
- OCTAVE^{SM} (Operationally Critical Threat, Asset, and Vulnerability Evaluation^{SM}) Method Implementation Guide Version 2.0, Carnegie Mellon – Software Engineering Institute, Pittsburgh, PA 15213-3890, http://www.cert.org/octave/ - septiembre de 2004.
- POBLACIÓN, Martín; apuntes de "Seguridad Informática", Universidad Empresarial Siglo 21, marzo de 2003.

- SYNC TECHNOLOGIES; “Glosario de Siglas”; http://www.sync.com.ar/sync/siglas/ - mayo de 2005.
- The SANS Institute; 8120 Woodmont Avenue, Suite 205 Bethesda, Maryland 20814, http://www.sans.org/ - marzo de 2005
- VIRUSPROT.COM; “Glosario”; http://www.virusprot.com/Glosarioc.html - mayo de 2005.
- YOUNG BARBÉ, Guillermo; trabajo “Análisis sobre la aplicación de aspectos de seguridad a equipos informáticos SCADA (Sistemas de Control y Adquisición de Datos)”, materia Práctica Profesional, Universidad Empresarial Siglo 21, julio de 2003.