POLITICAS DE SEGURIDAD INFORMÁTICA (PSI)

Departamento de Tecnología Organización Inca

CONTENIDO

Pág.

INTRODUCCIÓN

Sres. Directores, la información es el principal activo de nuestra empresa, la vulnerabilidad de nuestros sistemas de información requiere establecer los mecanismos necesarios para salvaguardar los datos de la compañía que pueden originar su perdida por mal manejo de la información, e inclusive por personas con malas intenciones. Perder información parcial o total e inclusive que caiga en manos de nuestra competencia pueden representar una enorme pérdida en los ingresos y utilidades originados por la pérdida de clientes y cartera. El desarrollo de una PSI nos van ayudar a salvaguardar ese activo tan importante.

1. GENERALIDADES.

La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles. La posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información.

Estos riesgos que se enfrentan, ha llevado a que muchas desarrollen documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de las mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la empresa.

En este sentido, las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y servicios críticos que permiten a la empresa crecer y mantenerse competitiva. Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades , y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodeas las organizaciones modernas.

2. POLITICAS DE SEGURIDAD INFORMÁTICA

2.1. DEFINICIÓN

Una política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización.

No se puede considerar que una política de seguridad informática es una descripción técnica de mecanismos, ni una expresión legal que involucre sanciones a conductas de los empleados, es más bien una descripción de los que deseamos proteger y el porqué de ellos, pues cada política de seguridad es una invitación a cada uno de sus miembros a reconocer la información como uno de sus principales activos, así como un motor de intercambio y desarrollo en el ámbito de sus negocios. Por tal razón, las políticas de seguridad deben concluir en una posición consciente y vigilante del personal.

2.2. ELEMENTOS DE UNA POLITICA DE SEGURIDAD INFORMATICA.

Como una política de seguridad debe orientar las decisiones que se tomen en relación con la seguridad, se requiere la disposición de todos los miembros de la empresa para lograr una visión conjunta de lo que se considere importante.

Las políticas de Seguridad Informática deben considerar principalmente los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.

- Objetivos de la política y descripción clara de los elementos involucrados en su definición. Responsabilidades por cada uno de los servicios y recursos informáticos aplicados a todos los niveles de la organización.

- Requerimientos mínimos para la configuración de la seguridad de los sistemas que abarca el alcance de la política.

- Definición de violaciones y sanciones por no cumplir con las políticas.

- Responsabilidades de los usuarios con respecto a la información a la que tiene acceso.

Las políticas de seguridad informática, también deben ofrecer explicaciones comprensibles sobre porque deben tomarse ciertas decisiones y explicar la importancia de los recursos. Igualmente, deberán establecer las expectativas de la organización en relación con la seguridad y especificar la autoridad responsable de aplicar los correctivos o sanciones.

Otro punto importante, es que las políticas de seguridad deben redactarse en un lenguaje sencillo y entendible, libre de tecnicismo, términos ambiguos que impidan una comprensión clara de las mismas, claro está sin sacrificar su precisión.

Por último, y no menos importante, el que las políticas de seguridad, deben seguir unos procesos de actualización periódica sujeto a los cambios organizacionales relevantes, como son: El aumento de personal, cambios en la infraestructura computacional, alta rotación de personal, desarrollo de nuevos servicios, regionales de la empresa, cambio o diversificación del área de negocios, etc.

2.3. PARÁMETROS PARA ESTABLECER POLITICAS DE SEGURIDAD.

Es importante que al momento de formular las políticas de seguridad informática, se consideren por lo menos los siguientes aspectos:

- Efectuar un análisis de riesgo informáticos, para valorar los activos y así adecuar las políticas a la realidad de la empresa.

- Reunirse con los departamentos dueños de los recursos, ya que ellos poseen la experiencia y son la principal fuente para establecer el alcance y definir las violaciones a las prácticas.

- comunicar con todo el personal involucrado sobre el desarrollo de las políticas, incluyendo los beneficios, riesgos relacionados con los recursos, bienes, y elementos de seguridad.

- Identificar quien tiene la autoridad para tomar decisiones en cada departamento, pues son ellos los interesados en salvaguardar los activos críticos de su área.

- Monitorear periódicamente los procedimientos y operaciones de la empresa, que ante cambios, las políticas puedan actualizarse oportunamente.

- Detallar explicita y correctamente el alcance de las políticas con el propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad que respondan a las políticas trazadas.

2.4. PLAN DE TRABAJO PARA ESTABLECER POLITICAS DE SEGURIDAD.

- Agendar reunión con los coordinadores o jefes de departamentos.

- Destacar en que nos afecta a todos la perdida de información.

- Asumir el compromiso de las buenas prácticas en la manipulación de datos de la red informática.

- Establecer en la reunión las propuestas para definir las medidas de seguridad aplicadas a los coordinadores y personas a su cargo.

- Medidas de seguridad:

- Acceso a Internet

- Respaldo de la información

- Creación de grupos de usuarios de acurdo a su perfil

- Definir los permisos de acceso, escritura, lectura de archivos y carpetas de acuerdo al cargo asignado.

2.5. RECOMENDACIONES PARA IMPLANTAR LAS POLITICAS.

- Conocer los riesgos informáticos analizando los componentes físicos de la red y la manera como está organizada la información.

- Reunión con los jefes de departamentos que permitan valorar la información que manejan.

- Involucrar al personal de cada departamento explicando cuales son las ventajas de implementar PSI y los riesgos de no tenerla.

- Reconocer la responsabilidad de cada jefe de proceso de tal manera que tenga coincidencia y les quede claro las PSI.

- Establecer mecanismos que permitan auditar tanto los elementos físicos de la red como el desempeño de los usuarios.

3. PRIVACIDAD EN LA RED Y CONTROL DE INTRUSOS

3.1. Privacidad en la Red.

3.1.1. Generalidades.

Las comunicaciones son la base de los negocios modernos, pues sin las mismas ninguna empresa podría sobrevivir. Por tal razón, es necesario que las organizaciones mantengan sus servidores, datos e instalaciones lejos de los hackers y piratas informáticos.

La temática de la privacidad de las redes ha ido cobrando, desde hace más de una década, un lugar bien importante en el entorno del desarrollo de la informática, ya que las empresas se sienten amenazadas por el crimen informático y busca incasablemente tecnologías que la protejan del mismo, para lo cual destinan partidas en sus presupuestos para fortalecer la seguridad de la información y las comunicaciones.

El mantener una red segura, fortalece la confianza de los clientes en la organización y mejora su imagen corporativa, ya que muchos son los criminales

informáticos (agrupaciones profesionales, aficionadas y accidentales) que asedian día a día las redes. De forma cotidiana estos hackers aportan novedosas técnicas de instrucción, códigos malignos más complejos y descubren nuevos vacíos en las herramientas de software.

3.2. DEFINICION DE PRIVACIDAD DE LAS REDES

Las redes son sistemas de almacenamiento, procesamiento y trasmisión de datos que están compuestos de elementos de trasmisión (cables, enlaces inalámbricos, satélites, encaminadores, pasarelas, conmutadores, etc.), y servicios de apoyo (sistemas de nombre de dominio incluidos los servidores raíz, servicio de identificación de llamadas, servicio de autenticación, etc.).

Conectadas a las redes existe un número cada vez mayor de aplicaciones (sistemas de entrega de correo electrónico, navegadores, etc.) y equipos terminales (Servidores, teléfonos, computadores personales, teléfonos móviles, etc.).

Las redes en las empresas, son los medios que permiten la comunicación de diversos equipos y usuarios, pero también están propensas a ser controladas o acezadas por personas no autorizadas. Cuando nos referimos a la privacidad de la red, se evoca al cuidado o medida establecida para que la información de los sistemas como puede ser datos del cliente, servicios contratados, reportes financieros y administrativos, estrategias de mercado, etc., no sea consultado por intruso.

3.3. REQUISITOS PARA MATENER LA PRIVACIDAD DE LAS REDES

Las redes deben cumplir los siguientes requisitos o características para mantener su privacidad y poder ser más seguros ante las posibilidades de intrusión.

1. **DISPONIBILIDAD**: significa que los datos son accesibles, inclusive en caso de alteraciones, cortes de corriente, catástrofes naturales, accidentes o ataques. Esta característica es particularmente importante cuando una avería de la red puede provocar interrupciones o reacciones en cadenas que afecten las operaciones de la empresa.

2. **AUTENTICACION**: confirmación de la identidad declarada de usuarios. Son necesarios métodos de autenticación adecuados para muchos servicios y aplicaciones, como la conclusión de un contrato en línea, el control de acceso a determinados servicios, la autenticación de los sitios web, etc.

3. **INTEGRIDAD**: confirmación de que los datos que han sido enviados, recibidos, almacenados son completos y no han sido modificados. La integridad es especialmente importante, en la relación con la autenticación de terminación de contratos o en casos que la exactitud de los datos es crítica.

4. **CONFIDENCIALIDAD**: Protección de las comunicaciones o los datos almacenados contra su interrupción y lectura por parte de personas no autorizadas. La confidencialidad es necesaria para la transmisión de datos sensibles y es uno de los requisitos principales a la hora de dar respuesta a las inquietudes en materia de intimidad de los usuarios de las redes de comunicación.

Es preciso tener en cuenta todos los factores que puedan amenazar la privacidad y no solamente los intencionados. Desde el punto de vista de los usuarios, los peligros derivados de los incidentes del entorno o de errores humanos que alteren la red pueden ser tan costosos como los ataques intencionados. La seguridad de las redes y la información. Puede entenderse como la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, todos los accidentes o acciones malintencionados, que pongan en peligro la disponibilidad, autenticidad y confidencialidad de los datos almacenados o transmitidos, de los correspondientes servicios que dichas redes y sistemas ofrecen o hacen accesibles.

3.4. RIESGOS O AMENAZAS A LA PRIVACIDAD DE LAS REDES.

Las principales amenazas o riesgos que enfrentan las empresas que utilizan las redes son:

1. **Interceptación de las Comunicaciones:** La comunicación puede ser interceptada y los datos copiados o modificados. La interceptación puede realizarse mediante el acceso físico a las líneas de las redes, por ejemplo, pinchado la línea, o controlando las transmisiones.

2. **Acceso no autorizado a ordenadores y redes de ordenadores:** El acceso no autorizado a ordenadores o redes de ordenadores se realiza habitualmente de forma malintencionada para copiar, modificar o destruir datos. Técnicamente, se conoce como intrusión y adopta varias modalidades: contraseñas previsibles, aprovechar la tendencia de la gente a desvelar información a personas en apariencia fiable e interceptación de contraseñas.

3. **Perturbación de las redes:** actualmente las redes se encuentran ampliamente digitalizadas por ordenadores, pero en el pasado la razón de perturbación de la red más frecuente era un fallo en el sistema que controla la red y los ataques a las redes estaban dirigidos principalmente a dichos ordenadores. En la actualidad, los ataques más peligrosos se concretan a los puntos débiles y más vulnerables de los componentes de las redes como son sistemas operativos, encaminadores, conmutadores, servidores de nombre de dominio, etc.

4. **Ejecución de programas que modifican y destruyen los datos:** los ordenadores funcionan con programas informáticos, pero lamentablemente los programas pueden usarse también para desactivar un ordenador y para borrar y modificar los datos. Cuando esto ocurre en un ordenador que forma parte de una red, los efectos de estas alteraciones pueden tener un alcance considerable. Por ejemplo, un virus en un programa informático malintencionado que reproduce su propio código que se adhiere, de modo que cuando se ejecuta el programa informático infectado se activa el código de virus.

   .

5. **Declaración falsa:** a la hora de efectuar una conexión a la red o recibir datos, el usuario formula hipótesis sobre la identidad de su interlocutor en función de contexto de la comunicación. Para la red, el mayor riesgo de ataque procede de la gente que conoce el contexto. Por tal razón, las declaraciones falsas de personas físicas o jurídicas pueden causar daños de diversos tipos. Como pueden ser, trasmitir datos confidenciales a personas no autorizadas, rechazo de un contrato, etc.

6. **Accidentes no provocados:** Numerosos accidentes de seguridad se deben a accidentes imprevistos o no provocados como: Son tormentas, inundaciones, incendios, terremotos, interrupción del servicio, por obras de construcción, defectos de programa y errores humanos o deficiencias de la gestión del operador, proveedor de servicio o el usuario.

NOTA:

Razones Que Impiden La Aplicación De Las Políticas De Seguridad Informática.

A pesar de que un gran número de organizaciones canalizan para definir directrices de seguridad y concentrarlas en documentos que orienten las acciones, de las mismas, muy pocas alcanzan el éxito, ya que la primera barrera que se enfrenta es convencer a los altos ejecutivos de la necesidad y beneficios de buenas políticas de seguridad informática.

Otros inconvenientes los representan los tecnicismos informáticos y la falta de una estrategia de mercadeo por parte de los Gerentes de Informática o los especialistas en seguridad.

Esta situación ha llevado a que muchas empresas con activos muy importantes, se encuentren expuestas a graves problemas de seguridad y riesgos innecesarios, que en muchos casos comprometen información sensitiva, por ende su imagen corporativa. Ante esta situación, los encargados de la seguridad deben confirmar que las personas entienden los asuntos importantes de la seguridad, conocen sus alcances y están de acuerdo con las decisiones tomadas en relación con esos asuntos.

Si se quiere que las políticas de seguridad sean aceptadas, deben integrarse a las estrategias del negocio, a su misión y visión, con el propósito de que los que toman las decisiones reconozcan su importancia e incidencias en las proyecciones y utilidades de la compañía.

Finalmente, es importante señalar que las políticas por si solas no constituyen una garantía para la seguridad de la organización, ellas deben responder a intereses y necesidades organizacionales basadas en la visión de negocio, que lleven a un esfuerzo conjunto de sus actores por administrar sus recursos y a reconocer en los mecanismos de seguridad informática factores que facilitan la formalización y materialización de los compromisos adquiridos con la organización.

4. NORMAS Y PROCEDIMIENTOS.

Al igual que en todas las organizaciones y partes que la conforman, el departamento de Sistemas debe tener una serie de Normas y Procedimientos que rijan el comportamiento tanto de los empleados que ahí laboran como de los que hacen uso de las facilidades que este departamento les proporciona; a continuación presentamos dichas Normas y Procedimientos.

4.1. Reglamento Interno.

1. Todos los empleados del departamento deberán presentarse diariamente a sus labores.
2. El horario que deben cumplir es de lunes a sábado
3. Todos los practicantes deben checar su entrada en el programa de horario que se encuentra en la red local de la empresa.
4. Deberán mantener limpio y en buen estado sus lugares de trabajo.
5. El teléfono es para cuestiones de trabajo, por lo que se debe utilizar lo menos posible en asuntos personales.
6. Cada vez que algún practicante deba salir del departamento, es necesario que notifique a la secretaria.
7. El equipo con el que labora cada empleado es responsabilidad suya, por lo que deberá cuidarlo y mantenerlo en buenas condiciones.
8. Somos un departamento de servicio por lo que es requisito que los practicantes tengan trato amable con los usuarios.
9. No se debe Fumar, Comer o Beber dentro del departamento.
10. Solo personal autorizado puede entrar a las áreas de trabajo.
11. Se llevaran a cabo reuniones interna en la que se revisarán los planes de trabajo así como las actividades desarrolladas y a desarrollar.
12. Debe existir un ambiente cordial de trabajo, por lo que en caso de haber algún mal entendido, sé deber aclarar inmediatamente, ya sea entre los involucrados o con la intervención del jefe de departamento.

4.2. Procedimientos.

Así como existen Normas para regular el funcionamiento del departamento internamente, existen algunos procedimientos que rigen la relación con las demás áreas de la empresa, cabe mencionar que solo se nombrarán aquellos que afectan directamente al departamento en relación con los demás.

4.2.1. Solicitud de Proceso.

Cada vez, que algún usuario o departamento requiere de una actividad por parte del departamento de sistemas podrá solicitarlo a este de una forma verbal (telefónica), siempre y cuando la actividad no requiera de muchos recursos de lo contrario deberá hacerlo a través de un correo electrónico o por la web de la organización.

4.2.2. Orden de Trabajo.

Todo técnico llevara una orden de trabajo para plasmar el trabajo realizado y quede la evidencia que se realizó.

4.2.3. Orden de Movilización.

En el momento de trasladar un equipo electrónico de un departamento a otro se deberá llenar una orden de movilización para tener la ubicación exacta del equipo o en algún caso que ingrese del exterior de la institución.

4.2.4. Seguridad.

Un punto muy importante dentro de un centro de cómputo y un Departamento de Sistemas es sin duda la seguridad, los activos y la información que ahí se manejan son tan críticos que cualquier daño que pudieran sufrir se convertiría en un gran desastre para la institución. Por ello, es de vital importancia implementar un procedimiento que regule precisamente este punto.

1. Controlar el acceso al área de Sistemas.
2. Utilizar antivirus actualizados.
3. Definir responsabilidades para la seguridad de datos, sistemas y programas.
4. Involucrar a varias personas en funciones delicadas. No depender de una sola para la realización de ellas.
5. Enfatizar al personal del departamento la importancia de la seguridad y su responsabilidad personal.
6. Establecer planes de contingencia y para casos de emergencia.
7. Dar a conocer solo al personal autorizado donde se encuentran y como obtener los datos confidenciales.
8. Mantener en buen estado los detectores de incendios, extinguidores y demás equipo para caso de incendio u otro desastre.
9. Proteger el equipo de daños físicos. (Polvo, humo, etc.)
10. Alejar todo material magnético dado que puede dañar las unidades de almacenamiento.
11. Cambiar claves de acceso con regularidad.
12. Tener y llevar a cabo un plan de respaldos.
13. Mantener el área limpia y ordenada.

14. Utilizar reguladores, acondicionadores y baterías para cambios de corriente.

5. FUNCIONES DEL DEPARTAMENTO.

5.1. Principales funciones y servicios que ofrece.

La principal función de un Departamento de Sistemas es crear y ofrecer sistemas de información que permitan dar solución a las necesidades informáticas y de toma de decisiones de la institución.

Es necesario destacar que nosotros como departamento de Sistemas, somos un departamento de servicio, y que nuestros clientes son precisamente los demás departamentos que conforman el grupo. Los productos que nosotros ofrecemos son servicios y se pueden agrupar en las siguientes funciones:

1. La administración y mantenimiento de los sistemas existentes en el grupo
2. Asesoría y capacitación a los diferentes departamentos y empresas del grupo.
3. Estudios de factibilidad, compra e instalación de equipo.
4. Evaluación, adquisición de software y paquetería.
5. Desarrollo de nuevos sistemas.
6. Elaboración de manuales y documentación.
7. Administración, mantenimiento de Pc, Redes y equipo.
8. Revisión periódica de las necesidades de información.
9. Contratación de servicios y asesorías externas.
10. Mantenimiento y reparación de equipo de cómputo.
11. Implementación, administración de los servicios de Internet y correo electrónico.

6. METAS Y OBJETIVOS

El objetivo básico del Departamento de Sistemas consiste, en suministrar la información que se necesita para controlar la estrategia y llevar a cabo las diferentes funciones de la empresa, así como de las herramientas necesarias para su manipulación.

- ✓ Constituir el grupo como una sola institución e implementar un sistema de información único que funcione para todas las áreas.
- ✓ Estandarizar los equipos y sistemas.
- ✓ Mantenernos como un departamento líder en los servicios que ofrecemos.

7. CONCLUSIONES

Es un hecho que un Departamento de Sistemas es un departamento de servicios, que sus clientes son los propios empleados y áreas de la empresa, que son los que ocupan sus servicios, los cuales, son importantes, como los que se le ofrecen a los clientes externos; porque aunque erróneamente se crea que un departamento de servicios solo ocasiona gastos y no genera ingresos, estos últimos están implícitos en los ahorros que promueve y que logra a través de un adecuado manejo de la información.

8. BIBLIOGRAFIA

NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC 27001

es un estándar para la seguridad de la información (*Information technology - Security techniques - Information security management systems - Requirements*) aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.

Esta especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI).

DEPARTAMENTO DE TECNOLOGIA – CENTRO INCA
Rubén Rodríguez – José Ribón Zarco