Resumen Rolando

TEORÍA GENERAL DE LOS SISTEMAS

SISTEMAS

El concepto SISTEMAS ha invadido todos los campos de la ciencia y penetrado en el pensamiento y el habla populares y en los medios de comunicación.

El razonamiento en términos de sistemas desempeña un papel dominante en muy variados campos científicos.-

Se hizo necesario, pues, un “enfoque de sistemas”.

Dado un determinado objetivo, encontrar caminos o medios para alcanzarlo requiere que el especialista en sistemas (o el equipo de especialistas) considere soluciones posibles y elija las que prometen optimización, con máxima eficiencia y mínimo costo en la TOTALIDAD DEL PROBLEMA.

Visión Holística

Un sistema se define como una entidad con límites y con partes interrelacionadas e interdependientes cuya suma es mayor a la suma de sus partes.

La teoría general de sistemas en su propósito más amplio, contempla la elaboración de herramientas que capaciten a otras ramas de la ciencia en su investigación práctica.

Por sí sola, no demuestra ni deja de mostrar efectos prácticos.

La TGS es el contexto adecuado que permitirá dar soporte a una nueva explicación, que permitirá poner a prueba y verificar su exactitud.

Por esto se la ubica en el ámbito de las metateorías.

HOLÍSTICO

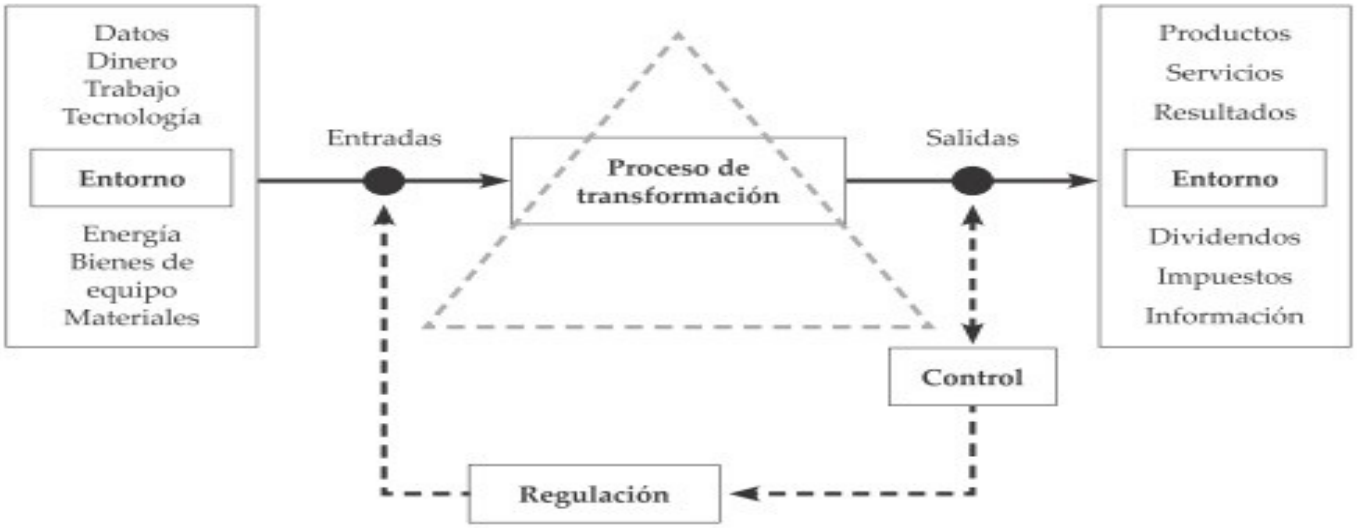
La **posición metodológica y epistemológica** llamada holística postula que la manera de hacerlo debería ser tomando el todo como objeto de estudio de un sistema y no sólo a partir de sus partes conformantes.

La palabra *holismo* **significa *todo, totalidad, por entero***. Según este método de estudio se debe tomar a los sistemas físicos, biológicos, económicos, mentales, lingüísticos, sociales, etcétera, como totalidades y analizar el todo junto a las características del sistema y no sólo remitirse a las partes.

Un sistema es mucho más que la simple suma de las partes, por eso es que este método de estudio considera el sinergismo de las partes como importante y no la individualidad de las mismas.

Como opuesto a la holística (o filosofía holista) se encuentra el reduccionismo**,** que sostiene que un sistema puede ser explicado y estudiado a partir de las partes que lo componen. Desde el punto de vista de las ciencias sociales, también **se opone a la holística el individualismo metodológico.**

La Organización como un Sistema



La Administración una Herramienta Útil

La Importancia de la Herramienta

La administración es una actividad indispensable en cualquier organización, de hecho es la manera más efectiva para garantizar el éxito de los proyectos.

Existen diversos conceptos de administración, coloquialmente se dice que: “administración es hacer algo a través de otros”.

Otra acepción es lo que se conoce como la “ley de oro de la administración”, entendida como hacer más con menos. Para entender el proceso de administración basta con analizar en qué consisten cada uno de los elementos indispensables en su gestión:

PLANIFICAR

La planeación es la determinación del rumbo hacia el que se dirige el PROYECTO y los resultados que se pretende obtener mediante el análisis del entorno y la definición de estrategias para minimizar riesgos tendientes a lograr OBJETIVO una mayor probabilidad de éxito.

ORGANIZAR E INTEGRAR LOS RECURSOS

La organización consiste en el diseño y determinación de las estructuras,procesos, sistemas,métodos y procedimientos tendientes a la simplificación y optimización del trabajo para alcanzar los OBJETIVOS.

La integración es la función a través de la cual se eligen y obtienen los recursos necesarios para poner en marcha las decisiones requeridas para ejecutar los planes de acuerdo con las necesidades.

DIRECCIÓN

La dirección es la EJECUCIÓN de los planes de acuerdo con la estructura organizacional, mediante la guía de los esfuerzos del grupo laboral a través de la motivación,la comunicación y el ejercicio del liderazgo.

CONTROL

La evaluación y control es la fase del proceso administrativo a través de la cual se establecen los estándares para medir los resultados obtenidos con el fin de corregir desviaciones, prevenirlas y mejorar continuamente el desempeño del equipo de trabajo.

Normas ISO

International Organization for Standardization
Organización Internacional para la Estandarización objetivos fundamentales: simplificar la coordinación internacional unificar los estándares industriales

ISO como organización única a nivel internacional para la normalización.

Actualmente la organización internacional de normalización acoge a 165 países miembros y lo conforman alrededor de 3368 órganos técnicos encargados de cuidar la elaboración de dichas normas.

La palabra ISO, significa según su raíz griega “igual”, de ahí el nombre de la organización, que además, coincide con las siglas de la misma.

Se trata de un juego de palabras muy adecuado para la finalidad de la organización.

Esta es una federación internacional independiente que intenta aportar mayor seguridad, calidad y eficiencia a los sistemas de trabajo para hacer más simple el intercambio entre países y regiones de bienes y servicios producidos.

Cada país tiene su propio organismo nacional de normalización de tipo no gubernamental que se puede ver como un puente de contacto entre el sector público y el sector privado. Normas IRAN

Los miembros son parte de la estructura de gobierno de cada país al que pertenecen pero también existen miembros que tienen raíces no gubernamentales ya que provienen del sector privado únicamente.

Por ello, las normas de la ISO permiten llegar a consensos sobre las posibles soluciones de cara a los negocios como para el beneficio general de la sociedad, en un ámbito más amplio.

- ISO 9001 para los Sistemas de Gestión de la Calidad.
- ISO 14001 para los Sistemas de Gestión Ambiental.
- ISO 27001 para los Sistemas de Gestión de Seguridad de la Información.
- ISO 31000 para los Sistemas de Gestión de Riesgos.

INTRODUCCIÓN

Esta Norma ha sido elaborada para suministrar requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información.

El establecimiento e implementación del sistema de gestión de la seguridad de la información de una organización están influenciados por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizacionales empleados, y el tamaño y estructura de la organización.

OBJETO Y CAMPO DE APLICACIÓN

Esta Norma especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información dentro del contexto de la organización.

Además incluye los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información, adaptados a las necesidades de la organización. Los requisitos establecidos en esta Norma son genéricos y están previstos para ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza.

¿Por qué es Importante para su Empresa?

Hay 4 ventajas comerciales esenciales que una empresa puede obtener con la implementación de esta norma para la seguridad de la información:

- Cumplir con los requerimientos legales.
- Obtener una ventaja comercial.
- Menores costos.
- Una mejor organización.

METODOLOGÍA

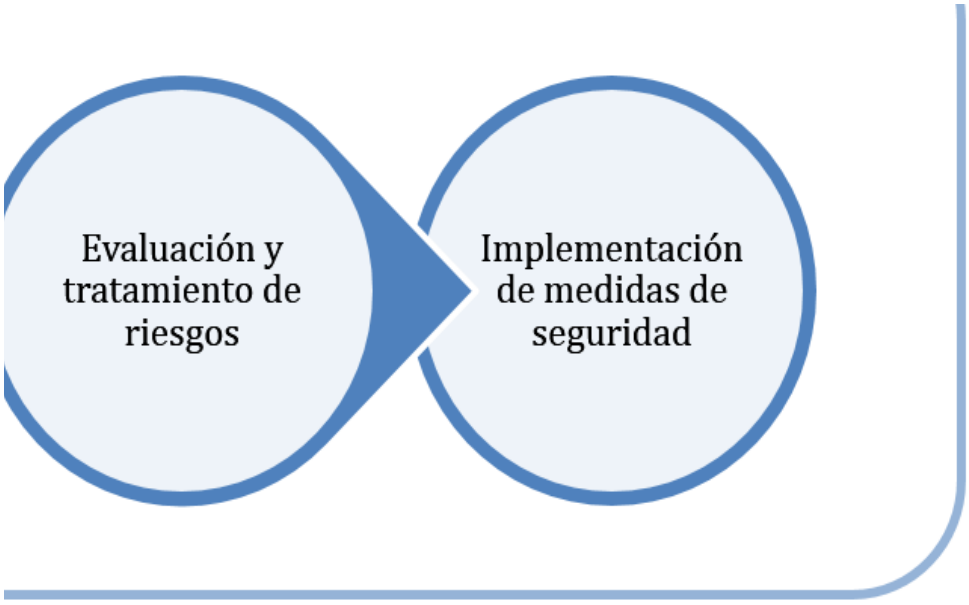
ESTRUCTURA DE LA NORMA

GESTIÓN DE RIESGOS

Normas ISO

Son un conjunto de normas orientadas a ordenar la gestión de una empresa en sus distintos ámbitos

Se crearon con la finalidad de ofrecer orientación, coordinación, simplificación y unificación de criterios a las empresas y organizaciones con el objeto de reducir costes y aumentar la efectividad, así como estandarizar las normas de productos y servicios para las organizaciones internacionales.



Gestión del Riesgo

Conceptos

Gestión de Riesgo en la Seguridad Informática: es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo.

Seguridad Informática sirve para la protección de la información, en contra de amenazas, para evitar daños y para minimizar riesgos, relacionados con ella.

Sistema de Gestión de la Seguridad de la Información El SGSI es el concepto sobre el que se construye ISO 27001.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Datos: es una representación simbólica de una variable cuantitativa o cualitativa.

Información: es toda aquella documentación en poder de una organización e independientemente de la forma en que se guarde o transmita (escrita, representada mediante diagramas o impresa en papel, almacenada electrónicamente, proyectada en imágenes, enviada por fax o correo, o, incluso, transmitida de forma oral en una conversación presencial o telefónica), de su origen (de la propia organización o de fuentes externas) y de la fecha de elaboración.

La seguridad de la información consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

Así pues, **estos tres términos constituyen la base** sobre la que se cimienta todo el edificio de la seguridad de la información:

Confidencialidad: acceso a la información por parte únicamente de quienes estén autorizados.

Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

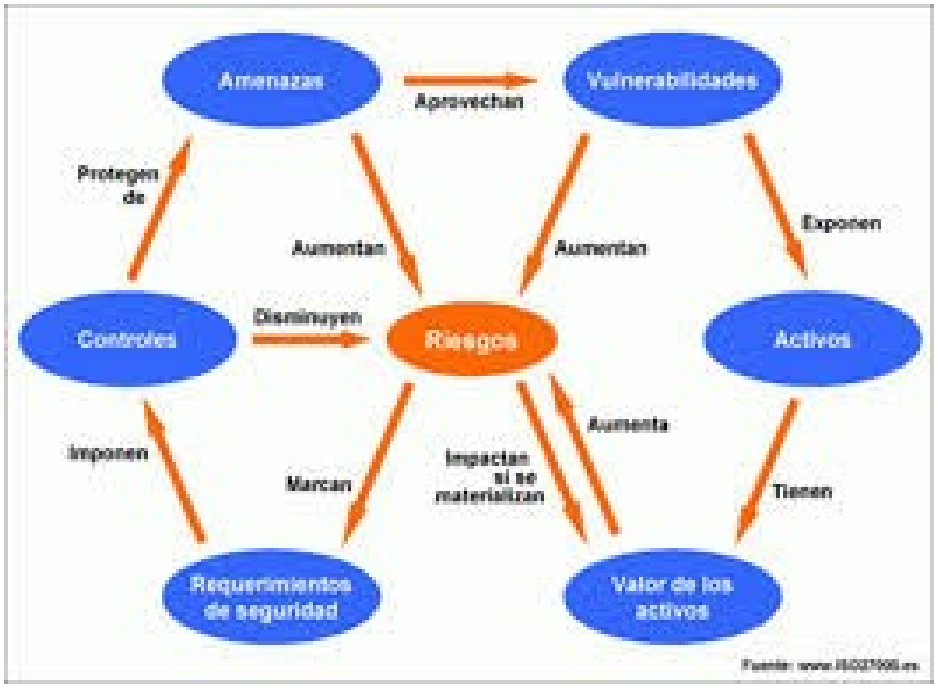
Disponibilidad: Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.

ACTIVO: son los recursos del sistema de información o relacionados con éste, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección. El activo esencial es la información.

AMENAZA: es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema.

VULNERABILIDAD: es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño.

SE DENOMINA RIESGO: A LA MEDIDA DEL DAÑO PROBABLE SOBRE UN SISTEMA.



SGSI

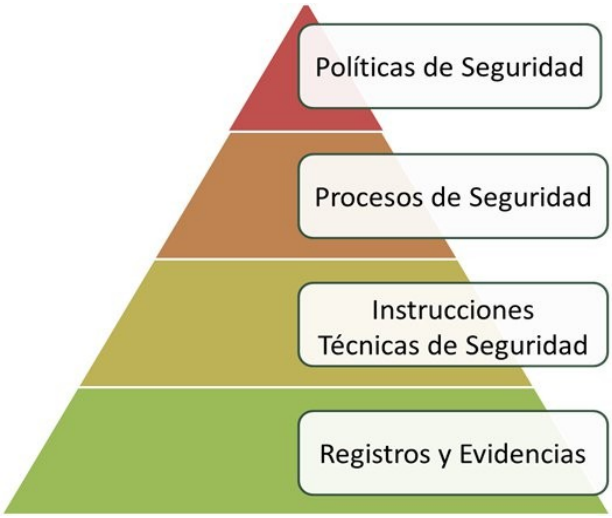
Con un SGSI, **la organización conoce los riesgos** a los que está sometida su información y los asume, **minimiza, transfiere o controla** mediante una sistemática definida, documentada y conocida por todos, que se revisa y actualiza constantemente.

¿Qué incluye un SGSI? Un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001 está formado por una serie de documentos que pueden clasificarse en una pirámide de cuatro niveles.

¿Cómo se implementa un SGSI?

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, **se utiliza el ciclo continuo PDCA,** tradicional en los sistemas de gestión de la calidad.

- **Plan** (planificar): establecer el SGSI.
- **Do** (hacer): implementar y utilizar el SGSI
- **Check** (verificar): monitorizar y revisar el SGSI.
- **Act** (actuar): mantener y mejorar el SGSI.



Plan: Establecer el SGSI

Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión

- **Definir una metodología de evaluación del riesgo**
- **Identificar los riesgos**
- **Analizar y evaluar los riesgos**

Do: Implementar y utilizar el SGSI

- **Definir un plan de tratamiento de riesgos**
- **Implantar el plan de tratamiento de riesgos**
- **Implementar los controles anteriormente seleccionados**
- **Definir un sistema de métricas que permita obtener resultados reproducibles**
- **Procurar programas de formación y concienciación**
- **Gestionar las operaciones del SGSI.**

- **Gestionar los recursos**

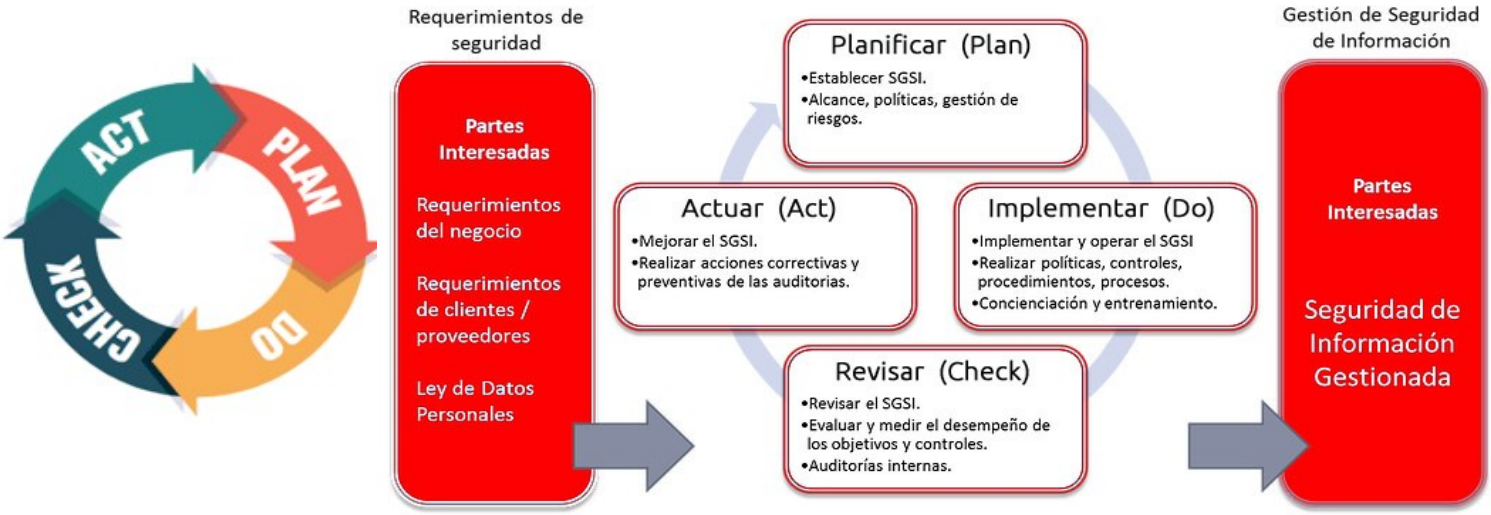
Check: Monitorizar y revisar el SGSI

- **Ejecutar procedimientos de motorización y revisión**
- **Revisar regularmente la efectividad del SGSI,**
- **Medir la efectividad de los controles**
- **Realizar periódicamente auditorías internas del SGSI**
- **Actualizar los planes de seguridad**
- **Registrar acciones y eventos**

Act: Mantener y mejorar el SGSI

- **Implantar en el SGSI las mejoras identificadas.**

- **Realizar las acciones preventivas y correctivas**
- **Comunicar las acciones y mejoras a todas las partes interesadas**
- **Asegurarse que las mejoras introducidas alcanzan los objetivos previstos**.



Análisis de Riesgo

Permite ubicar el riesgo y conocer los factores que influyen, negativa- o positivamente, en el riesgo.

En el proceso de analizar un riesgo también es importante de reconocer que cada riesgo tiene sus características:

- Dinámico y cambiante (Interacción de Amenazas y Vulnerabilidad)
- Diferenciado y tiene diferentes caracteres (caracteres de Vulnerabilidad)
- No siempre es percibido de igual manera en una institución

ACTIVOS

Se denominan activos los recursos del sistema de información o relacionados. El activo esencial es la información que maneja el sistema; o sea los datos.

- Los servicios que se necesitan para poder gestionar dichos datos.
- Las aplicaciones informáticas (software) que permiten manejar los datos.
- Los equipos informáticos (hardware) y que permiten hospedar datos, aplicaciones y servicios.
- Las redes de comunicaciones que permiten intercambiar datos.
- Las instalaciones que acogen equipos informáticos y de comunicaciones.
- Las personas que explotan u operan todos los elementos anteriormente citado

Valoración → ¿Por qué interesa un activo X lo que vale?

No se está hablando de lo que cuestan las cosas, sino de lo que valen. Si algo no vale para nada, prescíndase de ello. Si no se puede prescindir impunemente de un activo, es que algo vale; Eso es lo que hay que averiguar pues eso es lo que hay que proteger

Valores Cuantitativos y/o Cualitativos

El modelo se puede aplicar a los diferentes elementos de manera aislado, pero es sumamente importante aplicarlo también al sistemas completa,

Entre más alta la Probabilidad de Amenaza y Magnitud de Daño, más grande es el riesgo y el peligro al sistema, lo que significa que es necesario implementar mayores medidas de protección.

Existen varios métodos de como valorar un riesgo y al final, todos tienen los mismos retos -las variables son difíciles de precisar y en su mayoría son estimaciones- y llegan casi a los mismos resultados y conclusiones.

En el ámbito de la Seguridad Informática, el método más usado es el Análisis de Riesgo. La valoración del riesgo basada en la fórmula matemática:

Riesgo = Probabilidad de Amenaza x Magnitud de Daño

¿Cuánto vale la “salud” de los activos?

La valoración es la determinación del coste que supondría salir de una incidencia que destrozara el activo.

Hay muchos factores a considerar:

• **coste de reposición**: adquisición e instalación

• **coste de mano de obra** (especializada) invertida en recuperar el activo

• **lucro cesante**: pérdida de ingresos

• **capacidad de operar**: confianza de los usuarios y proveedores

• **sanciones por incumplimiento de la ley** u obligaciones contractuales

• **daño a otros activos,** propios o ajenos **• daño a personas**

Valoración cualitativa

Las escalas cualitativas permiten avanzar con rapidez, posicionando el valor de cada activo en un orden relativo respecto de los demás.

Es frecuente plantear estas escalas como “órdenes de magnitud” y, en consecuencia, derivar estimaciones del orden de magnitud del riesgo.

La limitación de las valoraciones cualitativas es que no permiten comparar valores más allá de su orden relativo.

No se pueden sumar valores.

Valoración cuantitativa

Las valoraciones numéricas absolutas cuestan mucho esfuerzo;

pero no adolecen de los problemas de las valoraciones cualitativas.

Sumar valores numéricos es absolutamente “natural” y la interpretación de las sumas no es nunca motivo de controversia.

Si la valoración es dineraria, además se pueden hacer estudios económicos • ¿Vale la pena invertir tanto dinero en esta salvaguarda? • ¿Qué conjunto de salvaguardas optimizan la inversión? • ¿En qué plazo de tiempo se recupera la inversión? • ¿Cuánto es razonable que cueste la prima de un seguro?

Las amenazas son “cosas que ocurren”.

Hay accidentes naturales (terremotos, inundaciones, …) **y desastres industriales** (contaminación, fallos eléctricos, …) ante los cuales el sistema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos.

Hay amenazas causadas por las personas,

- bien errores
- bien ataques intencionados.

No todas las amenazas afectan a todos los activos, sino que hay una cierta relación entre el tipo de activo y lo que le podría ocurrir.

Valoración de las amenazas

Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía.

Una vez determinado que una amenaza puede perjudicar a un activo, hay que estimar cuán vulnerable es el activo, en dos sentidos:

degradación: cuán perjudicado resultaría el activo

frecuencia: cada cuánto se materializa la amenaza

Determinación del impacto

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza.

Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

La única consideración que queda hacer es relativa a las dependencias entre activos.

Es frecuente que el valor del sistema de información se centre en los servicios que presta y los datos que maneja, al tiempo que las amenazas suelen materializarse en los medios.

Determinación del riesgo

Se denomina riesgo: **a la medida del daño probable sobre un sistema**.

Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la frecuencia de ocurrencia

- El riesgo crece con el impacto y con la frecuencia de ocurrencia

Salvaguardas

Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo.

Hay amenazas que se conjuran simplemente organizándose adecuadamente, otras requieren elementos técnicos (programas o equipos), **otras seguridad física** y, por último, **está la política de personal**.

Reduciendo la frecuencia de las amenazas. Se llaman salvaguardas preventivas. Las ideales llegan a impedir que la amenaza se materialice.

Hay salvaguardas que directamente limitan la posible degradación, **permiten detectar inmediatamente el ataque** para frenar que la degradación **permitir la pronta recuperación** del sistema cuando la amenaza lo destruye.

Oficina Nacional de Tecnologías de Información

Decálogo Tecnológico ONTI

Lineamientos y mejores prácticas para elaborar requerimientos de soluciones de tecnologías de la información y las comunicaciones en el Sector Público Nacional.

1. Conocé tu proyecto

2. Respetá las normativas y lineamientos

3. Preferí soluciones que utilicen la Nube

4. Utilizá estándares abiertos y soluciones interoperables

5. Elegí plataformas y soluciones comunes de Gobierno

6. Desarrollá soluciones reutilizables y compartilas

7. Asegurá que tus soluciones sean Accesibles

8. Protegé al sistema y a usuarios(as)

9. Garantizá disponibilidad y sustentabilidad en el tiempo

10. Asegurá una contratación conveniente y evitá la dependencia del oferente

1. Conocé tu proyecto

Conocé el alcance, evolución y escala del proyecto, las capacidades de tu equipo y las necesidades de los usuarios(as).

Ventajas

Los proyectos que contemplen todo el ciclo de vida son los que experimentan un mayor grado de adopción, ya que suelen satisfacer las necesidades de los usuarios(as) o ciudadanos(as) con mayor precisión, son más eficientes, sustentables y hacen un uso óptimo de los recursos públicos.

Lineamientos y mejores prácticas

● Definí el objetivo del proyecto (qué necesidad se resuelve), identificando usuarios(as), partes involucradas y sus necesidades.

● Identificá qué aspecto(s) claves se resuelve(n) o atiende(n) con este proyecto.

● Validá la existencia de un proyecto similar en la APN que se pueda reutilizar.

● Identificá el Ciclo de vida del proyecto (en meses o años). Considerá y organizá el proyecto por etapas. Para las etapas que no sean parte del alcance actual, se debe indicar al menos cuál es su objetivo y duración estimada.

● Determiná qué equipo de trabajo necesitás para tu proyecto y si contás con el mismo en tu organismo, cumpliendo con los objetivos de equidad de género.

● Justificá el dimensionamiento de tu proyecto basado en datos concretos de la implementación de la solución en tu organización.

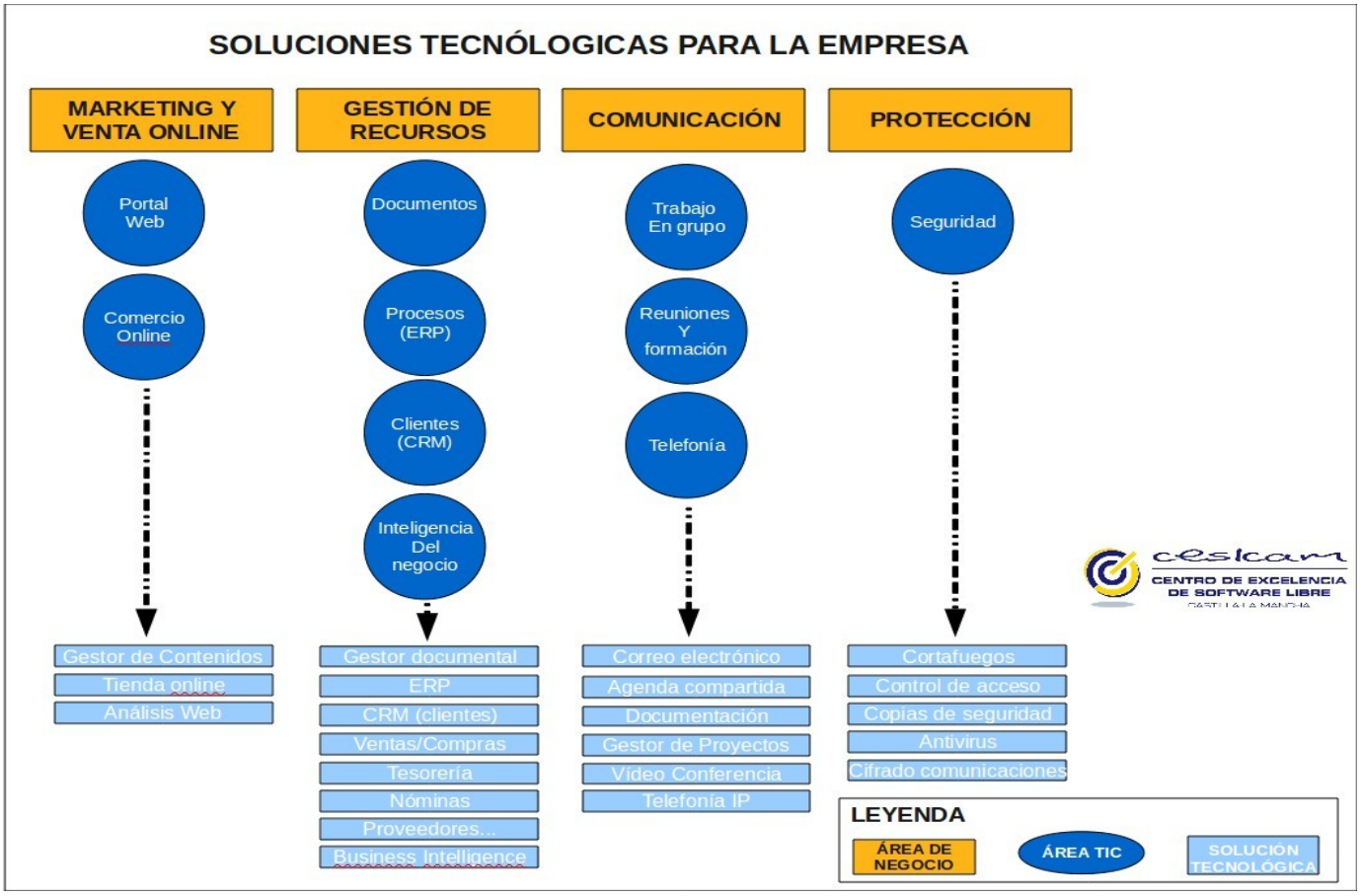
● Estimá el costo total del proyecto. En caso de que se ejecute sólo una etapa, estimá el correspondiente a la etapa a ejecutar.

● Considerá en la implementación del proyecto, el ciclo presupuestario y la disponibilidad de partidas de tu organismo o de quien financie el mismo.

● Incorporá al proyecto mecanismos de monitoreo con indicadores que reflejen resultados “medibles” del avance de la implementación, del desempeño de la operación del mismo y del nivel de satisfacción del servicio con el usuario.

● Prevé la documentación del proyecto para facilitar su mantenimiento, seguimiento y reutilización.

● Indicá un(a) referente del proyecto que sea punto focal para todas las interacciones dentro y fuera del organismo.



2. **Respetá las normativas y lineamientos**

Respetá las normativas y lineamientos del Gobierno para que tu proyecto cumpla con normas y políticas, y sea sustentable en el largo plazo.

Ventajas

Las normativas, lineamientos y estándares ofrecen un marco referencial para el desarrollo e implementación de los proyectos en el SPN; son validadas al momento de emitir un dictamen en la ONTI, favoreciendo soluciones que satisfacen las necesidades de los usuarios y/o ciudadanos

Lineamientos y mejores prácticas

● Revisá qué Especificaciones técnicas de los ETAP(s) se ajustan a tu proyecto y utilizalas .

● Si no aplican las Especificaciones técnicas de los ETAP(s), revisá qué lineamientos y/o Modelos de Pliego pueden referirse a tu requerimiento.

● Conocé y cumpli con la Normativa y Disposiciones ONTI vigentes.

● Revisá si tu proyecto cumple con la Ley N° 26.653 de “Accesibilidad de la Información de las Páginas Web” y su normativa complementaria.

● Si se trata de Servicios Digitales para el Ciudadano(as), revisá que estén alineados con la normativa de Gobierno Digital.

● Publicá tu información según la Normativa y los principios de trabajo de Gobierno Abierto.

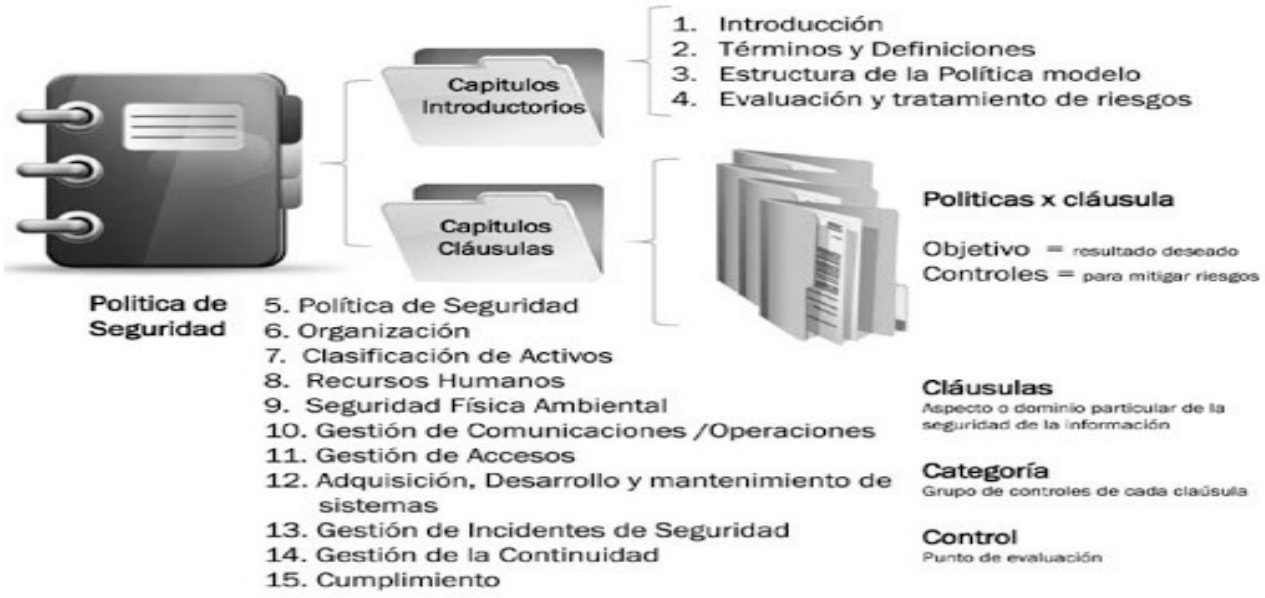
● Cumplí con la Normativa de la Secretaría de Modernización Administrativa.

● Considerá y preferí el uso de las soluciones de infraestructura que ofrece el Ministerio de Modernización (Ej. Usar el Data Center Benavidez antes de construir uno nuevo o expandir uno existente, Usar la Red MAN 2.0 para consumir servicios transversales de la APN o conectividad entre organismos, etc.)

● Catalogá -desde el inicio- la información y/o los sistemas de Información que tu proyecto utiliza para considerar el adecuado tratamiento y uso en la vida del mismo.

● Revisá el alineamiento de tu proyecto con las políticas TIC para la APN vigentes.

● Considerá en el desarrollo de tu solución los Lineamientos de nuevos conceptos Tecnológicos **para la innovación en áreas de gobierno que elabora la ONTI.**



3. Preferí soluciones que utilicen la Nube

Aprovechá las ventajas y soluciones que ofrece la Nube.

Gobierno identifica la “Nube híbrida” como el mejor escenario para cubrir todas las necesidades de infraestructura TIC en forma más eficiente.

Ventajas

El uso de la nube permite minimizar costos y gastos de mantenimiento, brindando a la vez escalabilidad y confiabilidad. La nube pública ofrece una amplia variedad de servicios, mientras que la nube privada ofrece un entorno controlado necesario para ciertas situaciones o requerimientos en ambientes de gobierno.

Lineamientos y mejores prácticas

● Los organismos de gobierno -al requerir servicios nuevos TI o crecer en existentes deben optar por soluciones en la Nube antes que por cualquier otra opción. ● Se identifica la “Nube Híbrida” (Nube Híbrida = Nube Privada y/o Nube Pública) como el mejor escenario para resolver todas las necesidades de infraestructura TIC de gobierno.

● Los organismos -a través de sus responsables- tendrán la decisión sobre la solución de Nube a contratar.

● Los proveedores de Servicios de Nube Pública que podrán ser utilizados por Gobierno deben cumplir con requisitos mínimos exigibles en su contratación.

4. Utilizá estándares abiertos y soluciones interoperables

Desarrollá tus soluciones utilizando estándares abiertos para maximizar la compatibilidad con otras plataformas, aumentar la transparencia y facilitar la colaboración.

Ventajas

La interoperabilidad y la utilización de estándares abiertos permiten la compatibilidad entre distintas tecnologías y ahorrar en costos de desarrollo o contratación de servicios. Además, facilita la colaboración entre organismos al mismo tiempo que fomenta la transparencia en la Administración Pública y la reducción de la dependencia de oferentes.

Lineamientos y mejores prácticas

● Utilizá sólo los estándares de la industria y evitá todo tipo de soluciones propietarias.

● Implementá soluciones basadas en protocolos y estándares globales.

● Exponé tus datos de interés público a través de una API.

● Documentá el código de tu aplicación o elaborá la documentación mínima necesaria para que tu solución sea fácil de entender, mantener y mejorar.

● Utilizá formatos de publicación de datos e información respetando los formatos abiertos e identificar la fuente canónica de cualquier información.

● Realizá los intercambios de información entre entidades y jurisdicciones del SPN de acuerdo a las “Pautas Técnicas de Interoperabilidad de Sistemas”.

5. Elegí plataformas y soluciones comunes de Gobierno

Recurrí a las soluciones de Gobierno disponibles para evitar la duplicación de esfuerzos, centralizar y homogeneizar el manejo de datos y optimizar la experiencia de los usuarios(as).

Ventajas

Utilizar las plataformas y soluciones de gobierno disponibles, evita la duplicación de esfuerzos a través de la centralización, reduciendo la diversificación de otras soluciones que puedan crear una dependencia de los oferentes. Además, permite unificar la experiencia con usuarios(as) para brindar un mejor servicio hacia los ciudadanos(as) de la República Argentina.

Lineamientos y mejores prácticas

● Utilizá las plataformas diseñadas por Gobierno Digital para atender a

Ciudadanos(as).

● Considerá cómo las Soluciones Transversales que Modernización Administrativa tiene implementadas y operando, pueden resolver ciertas problemáticas comunes en tu organismo.

● Utilizá las soluciones de Datos Abiertos para publicar en forma transparente y accesible la información de Gobierno.

● Conoce y verificá cómo las plataformas verticales pueden brindar solución a tus requerimientos tales como Telesalud o Id-Digital.

● Revisá las soluciones que País Digital ha implementado en Gobernaciones y Municipios, las de Nube Privada ofrecidas por el Data Center Benavidez del Ministerio de Modernización, o las de conectividad para la APN a través de la Red MAN 2.0.

6. Desarrollá soluciones reutilizables y compartilas

Diseñá tus soluciones para que sean reutilizables por otros organismos, para evitar la duplicación de esfuerzos y favorecer la colaboración.

Ventajas

Las soluciones que pueden ser reutilizadas por otros organismos optimizan el gasto público. Además, reutilizar soluciones potencia las interacciones entre equipos y facilita la mejora continua de las mismas.

Lineamientos y mejores prácticas

● Seguí los lineamientos de la Guía de Buenas Prácticas de Desarrollo de Software para la APN.

● Buscá soluciones existentes, desarrolladas por el Estado o no, antes de considerar iniciar un nuevo desarrollo.

● Comunicá tus necesidades a la Comunidad Digital AR para identificar posibles soluciones a tu necesidad.

● Colaborá con otros organismos y equipos en la implementación de soluciones reutilizables.

● Documentá tus soluciones para que sea más fácil su reutilización y adaptación.

SEGURIDAD DE LOS RECURSOS HUMANOS

La seguridad de la información se basa en la capacidad para preservar su integridad, confidencialidad y disponibilidad, por parte de los elementos involucrados en su tratamiento: equipamiento, software, procedimientos, así como de los recursos humanos que utilizan dichos componentes.

En este sentido, es fundamental educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de revista, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. De la misma forma, es necesario definir las sanciones que se aplicarán en caso de incumplimiento.

La implementación de la Política de Seguridad de la Información tiene como meta minimizar la probabilidad de ocurrencia de incidentes. Es por ello que resulta necesario implementar un mecanismo que permita reportar las debilidades y los incidentes tan pronto como sea posible, a fin de subsanarlos y evitar eventuales replicaciones. Por lo tanto, es importante analizar las causas del incidente producido y aprender del mismo, a fin de corregir las prácticas existentes, que no pudieron prevenirlo, y evitarlo en el futuro.

Objetivo

Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.

Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos de confidencialidad a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.

Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad del Organismo en el transcurso de sus tareas normales.

Establecer Compromisos de Confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información.

Alcance

Esta Política se aplica a todo el personal del Organismo, cualquiera sea su situación de revista, y al personal externo que efectúe tareas dentro del ámbito del Organismo.

Responsabilidad

El Responsable del Área de Recursos Humanos incluirá las funciones relativas a la seguridad de la información en las descripciones de puestos de los empleados, informará a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de usuarios respecto de la presente Política.

Categoría: Antes del empleo

Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados; y reducir el riesgo de robo, fraude y mal uso de los medios.

Las funciones y responsabilidades en materia de seguridad serán incorporadas en la descripción de las responsabilidades de los puestos de trabajo.

Éstas incluirán las responsabilidades generales relacionadas con la implementación y el mantenimiento de la Política de Seguridad, y las responsabilidades específicas vinculadas a la protección de cada uno de los activos, o la ejecución de procesos o actividades de seguridad determinadas.

Términos y condiciones de contratación

Como parte de sus términos y condiciones iniciales de empleo, los empleados, cualquiera sea su situación de revista, firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información del Organismo.

Asimismo, mediante el Compromiso de Confidencialidad el empleado declarará conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo.

Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado.

Se desarrollará un procedimiento para la suscripción del Compromiso de Confidencialidad donde se incluirán aspectos sobre sus alcances

Durante el empleo

Asegurar que los usuarios empleados, contratistas y terceras personas estén al tanto de las amenazas e inquietudes de la seguridad de la información, sus responsabilidades y obligaciones, y estén equipadas para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir el riesgo de error humano.

Se deben definir las responsabilidades de la gerencia para asegurar que se aplique la seguridad a lo largo de todo el tiempo del empleo de la persona dentro del Organismo.

Concientización, formación y capacitación en seguridad de la información

Todos los empleados del Organismo y, cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en el organismo, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos del Organismo. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo.

El Responsable del Área de Recursos Humanos será el encargado de coordinar las acciones de capacitación que surjan de la presente Política.

Adicionalmente, las áreas responsables de generar el material de capacitación dispondrán de información sobre seguridad de la Información para la Administración Pública Nacional en la Coordinación de Emergencias en Redes Teleinformáticas para complementar los materiales por ellas generados.

El personal que ingrese al Organismo recibirá el material, indicándosele el comportamiento esperado en lo que respecta a la seguridad de la información, antes de serle otorgados los privilegios de acceso a los sistemas que correspondan.

Por otra parte, se arbitrarán los medios técnicos necesarios para comunicar a todo el personal, eventuales modificaciones o novedades en materia de seguridad, que deban ser tratadas con un orden preferencial.

RELLENO de recurso humano

Continuando con los Dominios de la ISO 27002 (Numeral 8) o Anexo A de la ISO 27001 (Anexo A8), hoy vamos a revisar la Seguridad del Personal. Que dicen la ISO 27001 e ISO 27002? Bien, incluyen tres objetivos de control:

8.1 Antes de la contratación laboral

Asegurar que los empleados, contratistas y usuarios de terceras partes entienden sus responsabilidades y sean aptos para las funciones para las cuales están considerados, y reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones.

Las responsabilidades de la seguridad se deberían definir antes de la contratación laboral, describiendo adecuadamente el trabajo y los términos y condiciones del mismo.

Todos los candidatos para el empleo, los contratistas y los usuarios de terceras partes se deberían seleccionar adecuadamente, especialmente para trabajos sensibles.

Los empleados, contratistas y usuarios de terceras partes de los servicios de procesamiento de información deberían firmar un acuerdo sobre sus funciones y responsabilidades de seguridad

8.2 Durante la vigencia del contrato laboral

Asegurar que todos los empleados, contratistas y usuarios de terceras partes estén conscientes de las amenazas y preocupaciones respecto a la seguridad de la información, sus responsabilidades y deberes, y que estén equipados para apoyar la política de seguridad de la organización en el transcurso de su trabajo normal, al igual que reducir el riesgo de error humano.

- Se debería brindar un nivel adecuado de concientización, educación y formación en los procedimientos de seguridad y el uso correcto de los servicios de procesamiento de información a todos los empleados, contratistas y usuarios de terceras partes para minimizar los posibles riesgos de seguridad.

- Es conveniente establecer un proceso disciplinario formal para el manejo de las violaciones de seguridad.

8.3 Terminación o cambio de la contratación laboral

Asegurar que los empleados, los contratistas y los usuarios de terceras partes salen de la organización o cambian su contrato laboral de forma ordenada.

- Se deberían establecer responsabilidades para asegurar la gestión de la salida de los empleados, contratistas o usuarios de terceras partes de la organización y que se completa la devolución de todo el equipo y la cancelación de todos los derechos de acceso.

- Los cambios en las responsabilidades y las relaciones laborales dentro de la organización se deberían gestionar como la terminación de la respectiva responsabilidad o contrato laboral según esta sección y todas las contrataciones nuevas se deberían gestionar como se describe en el numeral 8.1

En pocas palabras, este es el propósito de la Norma:

La seguridad de los recursos humanos dentro de la organización, debe considerar como recurso humano al personal interno, temporal o partes externas en el aseguramiento de las responsabilidades que son asignadas a cada uno, asociadas con sus respectivos roles, para reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones.

Todo el recurso humano que hace parte de la Organización debe estar consciente de las amenazas y vulnerabilidades relacionadas con la seguridad de la información y sus responsabilidades y deberes en el apoyo que deben brindar a la política de seguridad de la organización establecida para la reducción del riesgo de error humano.

Profundizando en los requisitos de la Norma:

1 Seguridad antes de la contratación

Se deben realizar en conjunto con el área de recursos humanos una valoración del proceso de verificación de antecedentes que se debe aplicar al personal que ingrese a la Organización, teniendo en cuenta el tipo y clasificación de la información a la que tendría acceso en sus respectivos cargos y responsabilidades. Se debe tener en cuenta que no todos los procesos de contratación en la organización deben ser manejados de igual forma, cada rol y sus responsabilidades debe tener un manejo diferente con relación a la verificación de antecedentes, procedencia, formación, conocimientos, etc.

2 Seguridad durante la contratación

Se deben asegurar en la contratación del personal de la Organización, acuerdos de confidencialidad de la información que se manejarán durante el tiempo que labore dentro de la organización y una vez finalizado el contrato.

Debe quedar documentado en acuerdos de confidencialidad, materiales de concientización, contratos de empleo entre el empleado y la organización la responsabilidad de los trabajadores relacionada con la protección de la información manejada por la Organización.

Anualmente se debe considerar la posibilidad de revisar en conjunto con los empleados los términos, acuerdos y condiciones expuestas en los contratos laborales, para garantizar el compromiso que adquirieron con relación a la seguridad de la información con la organización.

3 Seguridad en la finalización o cambio de empleo

Cuando los empleados finalizan sus contratos laborales con la organización o se retiran de ésta, se deben tener en cuenta varias actividades que se deben realizar para garantizar la gestión apropiada de activos de la organización que tenía a su cargo.

El propósito fundamental de este Dominio de las la ISO 27002 ó Anexo A de la ISO 27001 es proteger la información de la organización inclusive desde antes de darle acceso a la misma a un tercero, sea este empleado, contratista, proveedor, etc.; así como durante toda la duración del contrato y su finalización, buscando evitar que cualquier persona que haya tenido acceso a la información por motivos laborales pueda darle un uso inadecuado a la misma. → Fin de relleno

ISO 27001 - Gestión Integral de Seguridad – SGSI

Se presenta un conjunto de gestiones que deberían definir e implementar las empresas para ir avanzando en el nivel de madurez de su modelo de seguridad de la información, teniendo como base:

- Los activos de información.
- Los riesgos de seguridad de la información.
- Los incidentes de seguridad de la información.
- El cumplimiento.
- La continuidad del Negocio.

- El cambio y cultura para la seguridad de la información.

- La Estrategia de seguridad de la información.

La norma internacional ISO/IEC 27001 ha sido presentada como un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de seguridad de la información, lo cual a priori nos indica que se puede generar un marco formal a través del cual se gestiona la seguridad de la información en las organizaciones.

Los esfuerzos realizados por las organizaciones para afrontar la problemática de la seguridad de la información, con relación a los riesgos que conlleva la pérdida de su confidencialidad, integridad o disponibilidad, ha llevado a que las mismas aumenten cada año sus inversiones para minimizar el nivel de su exposición al riesgo. Estas inversiones se traducen en proyectos que van desde una implementación tecnológica, que constituye un control de seguridad específico para la información, hasta proyectos tendientes a definir e implementar modelos de seguridad que permitan hacer una gestión continua de una estrategia de seguridad de la información, que debe implementarse y mejorase a través del tiempo.

La seguridad de la información es definida por la norma ISO/IEC 27001 como: “La Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad”, de otra forma, y en un sentido práctico, como elemento de valor al negocio, puede definirse como: “La protección de la información contra una serie de amenazas para reducir el daño al negocio y maximizar las oportunidades y utilidades del mismo”. Esta última definición nos sugiere con más fuerza que la seguridad de la información es un tema estratégico y de negocio que debe ser atendido desde la alta dirección.

En este sentido gestionar es coordinar y dirigir una serie de actividades, con recursos disponibles, para conseguir determinados objetivos, lo cual implica amplias y fuertes interacciones fundamentalmente entre el entorno, las estructuras, los procesos y los productos que se deseen obtener.

Teniendo en cuenta lo anterior, debemos reconocer que la gestión de la seguridad de la información requiere de una estrategia alineada con el negocio y sus objetivos, requiere de unos recursos y de un conjunto de actividades dirigidas y coordinadas por una organización de la seguridad que se extienda a través de toda la organización, desde la alta dirección hasta los usuarios finales.

Gestión de Activos de Información

En esta gestión se requiere identificar, valorar y clasificar los activos de información más importantes del negocio. Un activo de información en el contexto de un SGSI y con base en la norma ISO/IEC 27001 es: “algo a lo que una organización directamente le asigna un valor y por lo tanto la organización debe proteger”.

Se debe considerar como un activo de información principalmente a cualquier conjunto de datos creado o utilizado por un proceso de la organización., así como el hardware y el software utilizado para su procesamiento o almacenamiento, los servicios utilizados para su transmisión o recepción y las herramientas y/o utilidades para el desarrollo y soporte de sistemas de información. En casos particulares, se puede considerar como un activo de información a personas que manejen datos, transacciones, o un conocimiento específico muy importante para la organización (Por ejemplo: secretos industriales, manejo de claves importantes, “know how”).

1) **Inventario de Activos**: Todos los activos deben estar claramente identificados y se debe elaborar y mantener un inventario de todos los activos de información importantes de la organización.

Este inventario debe tener la valoración de cada activo, indicando bajo una escala definida por la organización, por ejemplo, si es de alto, medio, o bajo valor. Adicionalmente es importante que se indique cuáles son las propiedades más importantes de proteger para cada activo en términos de su Confidencialidad, Integridad y Disponibilidad, valorando cada propiedad. Se debe indicar cual es la ubicación del activo de información y cuales son los procesos que lo utilizan.

2) **Propiedad de los Activos:** Toda la información y los activos asociados con los servicios de procesamiento de información deben ser “propiedad” de una parte designada de la organización.

Propietario de la Información: El cual es una parte designada de la organización, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de definir quienes tienen acceso, que pueden hacer con la información, y de determinar cuales son los requisitos para que la misma se salvaguarde ante accesos no autorizados, modificación, pérdida de la confidencialidad o destrucción deliberada y al mismo tiempo de definir que se hace con la información una vez ya no sea requerida,

Custodio Técnico: Es una parte designada de la organización, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad (Toma de copias de seguridad, asignar privilegios de: Acceso, Modificaciones, Borrado) que el propietario de la información haya definido, con base en los controles de seguridad y recursos disponibles en la organización.

Usuario: Cualquier persona que genere, obtenga, transforme, conserve o utilice información de la organización en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la organización. Son las personas que utilizan la información para propósitos propios de su labor, y que tendrán el derecho manifiesto de su uso dentro del inventario de información.

Directrices de Clasificación: La información debe clasificarse en términos de su valor, de los requisitos legales, de su sensibilidad y la importancia para la organización.

Los niveles de clasificación de la información para cada organización pueden variar de alguna forma, y normalmente se establecen en términos de su confidencialidad, aunque puede establecerse un esquema tan completo que abarque niveles de clasificación por características de disponibilidad e integridad. Un esquema sencillo de clasificación, en términos de confidencialidad, puede manejar dos niveles, por ejemplo, información pública e información confidencial. Para otras organizaciones dos niveles pueden ser no suficientes y en cambio puede existir información: pública, de uso interno, confidencial y altamente confidencial.

Gestión de Riesgos de Seguridad de la Información

Esta gestión es un conjunto de actividades para controlar y dirigir la identificación y administración de los riesgos de seguridad de la información, para así poder alcanzar los objetivos del negocio. El riesgo es una característica de la vida de los negocios por lo cual hay que tener un control sobre los mismos.

La gestión de riesgos de seguridad de la información debe garantizar que el impacto de las amenazas que podrían explotar las vulnerabilidades de la organización, en cuanto a la seguridad de su información, estén dentro de los límites y costos aceptables

Gestión de Incidentes de Seguridad de la Información

Para comprender el objetivo de esta gestión hay que recurrir a las siguientes definiciones base:

Evento de seguridad de la información: un evento de seguridad de la información es la presencia identificada de un estado que indica un incumplimiento posible de la política de

seguridad de la información, una falla de los controles de seguridad, o una situación desconocida que puede ser pertinente para la seguridad de la información.

Incidente de seguridad de la información: un incidente de seguridad de la información está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de los activos de información. Los incidentes de seguridad de la información son hechos inevitables sobre cualquier ambiente de información, y estos pueden ser bastante notorios e involucrar un impacto fuerte sobre la información de la organización.

Gestión del Cumplimiento

Esta gestión permite identificar y administrar los riesgos de carácter jurídico que puede afrontar la organización, con respecto a incidentes presentados sobre sus activos de información, que se puede generar sobre diferentes componentes como son: comercio electrónico, protección de datos, habeas data, los incidentes informáticos y su connotación en términos de responsabilidad penal y civil, contratación informática y telemática, contratación laboral, contratación con terceros, derecho a la intimidad, la legislación propia del sector o industria, entre otros.

Lo que se busca es que se identifiquen los posibles riesgos que no han sido atendidos en las áreas legales antes mencionadas y para lo cual la empresa se podría encontrar vulnerable y a través de esta gestión atenderlos.

Gestión de la Continuidad del Negocio

Esta gestión desarrolla y administra una capacidad para responder ante incidentes destructivos y perjudiciales relacionados con la seguridad de la información que impidan continuar con las funciones y operaciones críticas del negocio, además debe tender por la recuperación de estos escenarios tan rápida y eficazmente como se requiera. Esta gestión debe permitir reducir el riesgo operacional de la organización.

Gestión del Cambio y Cultura para la seguridad

Esta gestión se enfoca a lograr un nivel alto de compromiso y actuación de todos los integrantes de la organización como parte fundamental del modelo de seguridad de la información. Esta gestión se convierte en un medio de vital importancia para difundir la estrategia de seguridad de la información a los diferentes niveles de la organización, para generar un cambio positivo hacia los nuevos papeles que entrarán a jugar las personas en la protección de los activos de información del negocio. El hecho de no tener un nivel adecuado de sensibilización en seguridad de la información deja en una situación de riesgo a la organización.

Gestión de la Estrategia de seguridad de la información

Para poder controlar y dirigir todas estas gestiones se hace necesario que la organización despliegue las mismas desde el más alto nivel de la organización, a través de:

Declaraciones Formales de Intención y Compromiso: Estas se materializan a través de políticas organizacionales que la alta dirección presenta a la organización (Por ejemplo: Política de seguridad de la información, o de la Información). Todos los demás niveles de documentación relacionados con la seguridad de la información a través de la organización, (Normas, Procedimientos, guías, etc) deben estar alineados y deben apoyar estas declaraciones de alto nivel, para que las mismas sean operativas y coherentes a través de las diferentes gestiones de seguridad.

Oportunidad de integración

En 1993, la ONU, en su Resolución “Normas estándar sobre la igualdad de oportunidades de las personas con minusvalía”, reconocía que las barreras del entorno constituyen obstáculos más graves a la participación social de las PCD que las limitaciones funcionales.

Hoy, se nos plantea el reto de mejorar la accesibilidad al trabajo a través de las TIC, que pueden aportar innumerables ventajas y nuevas oportunidades. En este sentido, la tecnología se ha lanzado al diseño de elementos que eliminen las barreras del entorno para que las PCD puedan desarrollarse como agentes productivos y, de este modo, mejorar su calidad de vida.

Esta revolución tecnológica está influyendo de manera fundamental en el incremento de las posibilidades de empleo de las PCD. Los desarrollos mitigan las dificultades derivadas de la reducción de la movilidad, la audición o la visión, posibilitando que las PCD utilicen su potencial cognitivo y se desempeñen en puestos de trabajo que antes les estaban vedados.

Diseño Universal

El “diseño universal”, también denominado “diseño para todos”, tiene la intención de incorporar las TIC al diseño de herramientas para que éstas sean lo suficientemente flexibles como para ser utilizadas sin ayudas técnicas complementarias por el mayor número posible de usuarios. Esto atañe a ingenieros, diseñadores, fabricantes y proveedores de servicios, y abarca sectores como el hardware, software, comercio electrónico, servicios públicos de información, Internet, servicios interactivos.

Tecnologías, productos y servicios

Las personas con poca fuerza o falta de coordinación en sus extremidades superiores encuentran dificultades en el manejo de los teclados o de un mause, que son los periféricos más comunes de acceso a las computadoras, mientras que las personas con problemas de audición o visión no pueden aprovechar la información en formato sonoro y visual. Pero cualquier tipo de discapacidad, tanto física como psíquica o sensorial, puede atenuarse a partir de las facilidades que aportan las nuevas tecnologías, productos y servicios.

Para esto existen las ayudas técnicas que son todos los productos, instrumentos, equipos o sistemas (de cualquier tipo de tecnología), accesibles para PCD, que mitigan o neutralizan la deficiencia o discapacidad, y mejoran la autonomía personal y la calidad de vida.

La tecnología al servicio de la calidad de vida

Además del plano laboral, resulta muy importante el papel desempeñado por las nuevas tecnologías en la reducción de las situaciones de dependencia y el incremento de la autonomía de las PCD.

Sin embargo, si bien las adaptaciones tecnológicas están suponiendo un gran avance, aún no son suficientes para cubrir todas las necesidades específicas de las personas con discapacidad.

Hay barreras de tipo económico y también formativo. Las PCD son mayoritariamente pobres a causa de sus deficiencias pero, también, en muchos casos, a pesar de contar con nivel adquisitivo suficiente, carecen de la formación necesaria para utilizar estas herramientas. La accesibilidad es otra barrera ya que, aun contando con recursos económicos y conocimientos para el uso, algunas PCD no pueden interactuar con estas herramientas por no estar adaptadas a su discapacidad particular.

El derecho al acceso

Lograr la accesibilidad digital es un mandato fundamental de la “Convención Sobre los Derechos de las Personas con Discapacidad” de las Naciones Unidas (2006). En relación con la accesibilidad, exponemos a continuación los siguientes lineamientos generales:

- Los servicios y facilidades públicas deben ser accesibles para todos.

- Las diferentes necesidades de las PCD deben ser tenidas en cuenta en el diseño de nuevos equipos y servicios.En caso de que el diseño universal no sea posible, las personas con discapacidad deberán poder acceder a los servicios por medio de equipos y servicios servicios adicionales o alternativos.

- Las personas con discapacidad deben poder utilizar los equipos y servicios a un costo lo más similar posible al de las personas sin discapacidad. Los costos del diseño universal no deben ser imputados sólo a las personas con discapacidad.

- Los proveedores de equipos y servicios, y las autoridades relevantes deben consultar a PCD sobre sus condicionantes y requerimientos de acceso antes de llevar a cabo alguna acción.

El libre acceso a las instalaciones y la facilidad de uso de los productos y servicios a menudo se da por sentado. Normalmente, sólo nos damos cuenta de lo importante que son cuando fallamos en el uso de algo. Pero las normas pueden ayudar! ISO, IEC e ITU acaban de publicar una nueva guía que asesora el desarrollo de normas sobre la manera de asegurarse de que sus normas tengan plenamente en cuenta las necesidades de accesibilidad de los usuarios de todos los ámbitos de la vida, y en particular de las personas con discapacidad, los niños y las personas mayores.

GUÍA ISO / IEC 71: 2014

Guía para abordar la accesibilidad en los estándares

ESTA NORMA FUE REVISADA Y CONFIRMADA POR ÚLTIMA VEZ EN 2021. POR LO TANTO, ESTA VERSIÓN PERMANECE ACTUALIZADA.

La Guía ISO / IEC 71: 2014 proporciona orientación a los desarrolladores de normas sobre cómo abordar los requisitos de accesibilidad y las recomendaciones en las normas que se centran, directa o indirectamente, en los sistemas (es decir, productos, servicios y entornos construidos) utilizados por las personas. Para ayudar a los desarrolladores de estándares a definir los requisitos y recomendaciones de accesibilidad, presenta un resumen de la terminología actual relacionada con la accesibilidad, cuestiones a considerar en apoyo de la accesibilidad en el proceso de desarrollo de estándares, un

conjunto de objetivos de accesibilidad (utilizados para identificar las necesidades de accesibilidad del usuario), descripciones de (y consideraciones de diseño para) las capacidades y características humanas, y estrategias para abordar las necesidades de accesibilidad de los usuarios y las consideraciones de diseño en los estándares.

El nuevo titulado Guía Guía para abordar la accesibilidad en las normas ayudarán a los involucrados en el proceso de desarrollo de normas para considerar los problemas de accesibilidad en el desarrollo o revisión de las normas, sobre todo en áreas donde no se han abordado antes. También será útil para los fabricantes, diseñadores, proveedores de servicios y los educadores con un interés especial en la accesibilidad.

Objetivos principales

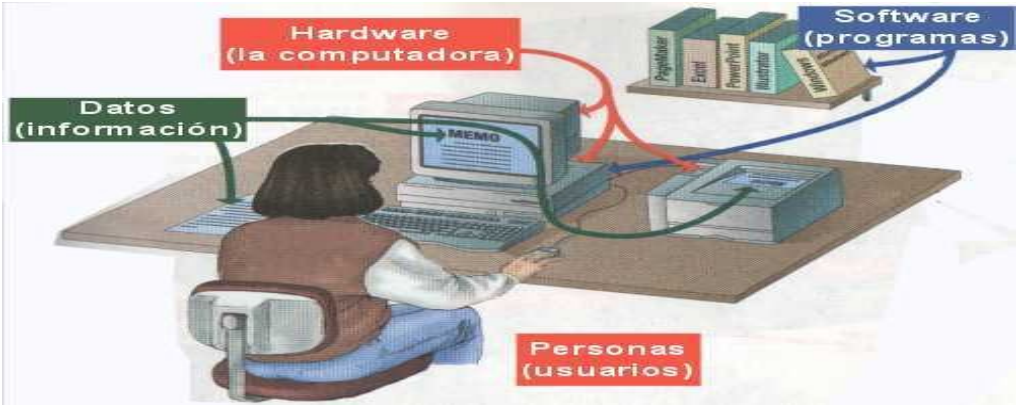
La nueva guía sobre la accesibilidad logrará fundamentalmente tres cosas:

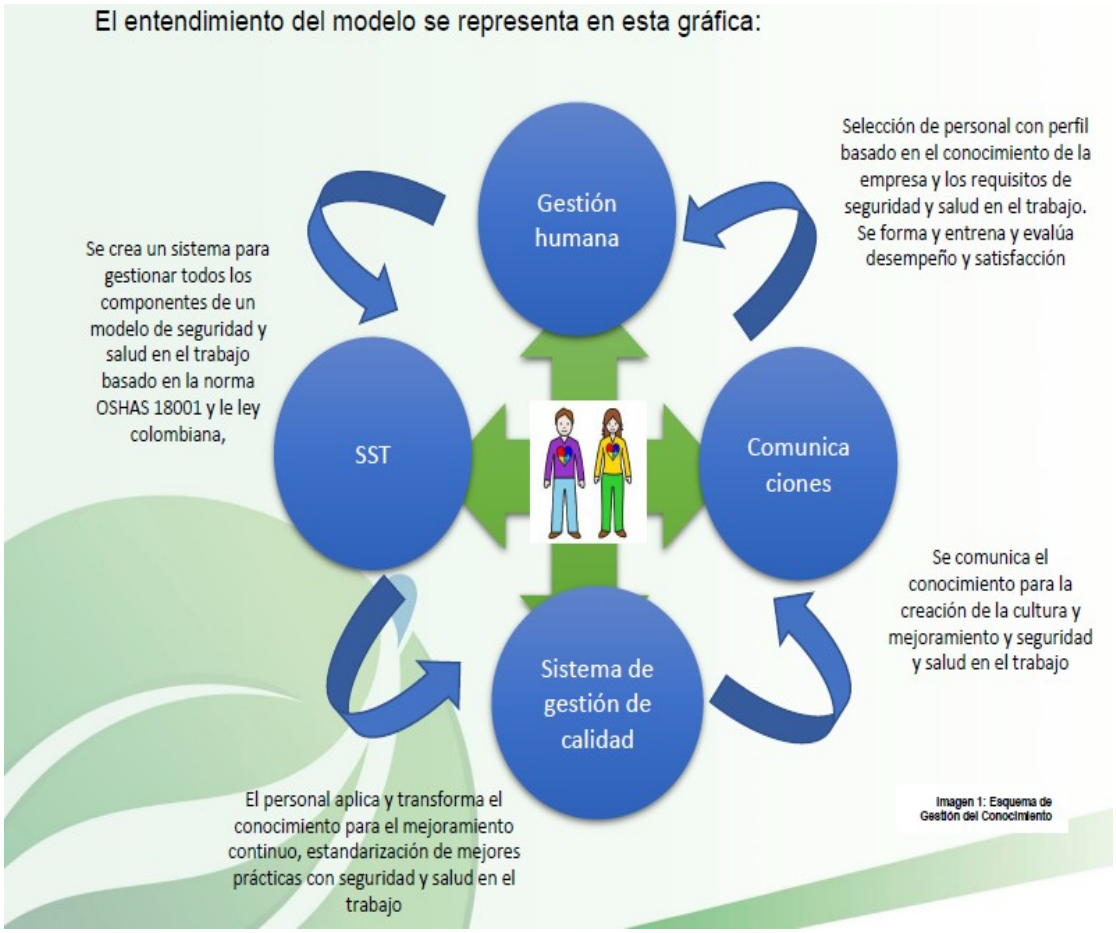
- **Ayudar** a los diseñadores, fabricantes y educadores a obtener una mejor comprensión de los requisitos de accesibilidad de nuestra creciente población

- **Aumentar** el número de normas que contienen las consideraciones de accesibilidad, tal vez con un número mayor se centra específicamente en la accesibilidad

- **Integrar** las funciones de accesibilidad en las normas - y el diseño del producto o servicio - Desde el comienzo

Seguridad en las Operaciones





La proliferación de software malicioso, como virus, troyanos, etc., hace necesario que se adopten medidas de prevención, a efectos de evitar la ocurrencia de tales amenazas. Es conveniente separar los ambientes de desarrollo, prueba y operaciones de los sistemas del Organismo, **estableciendo procedimientos que aseguren la calidad de los procesos** que se implementen en el ámbito operativo, a **fin de minimizar los riesgos de incidentes producidos por la manipulación de información operativa**. **Objetivo Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento**

Alcance Todas las instalaciones de procesamiento de información del Organismo.

El Responsable de Seguridad de la información tendrá a su cargo, entre otros:

- Definir procedimientos para el control de cambios a los procesos operativos documentados, los sistemas e instalaciones de procesamiento de información, y verificar su cumplimiento, de manera que no afecten la seguridad de la información.

- Establecer criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, contemplando la realización de las pruebas necesarias antes de su aprobación definitiva.

- Definir procedimientos para el manejo de incidentes de seguridad y para la administración de los medios de almacenamiento.

- Definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados en las redes

- Desarrollar procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.

El Responsable del Área Informática tendrá a su cargo lo siguiente:

- Controlar la existencia de documentación actualizada relacionada con los procedimientos de operaciones.

- Evaluar el posible impacto operativo de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando responsabilidades.

- Administrar los medios técnicos necesarios para permitir la segregación de los ambientes de procesamiento.

- Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad, a fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario.

- Controlar la realización de las copias de resguardo de información, así como la prueba periódica de su restauración.

- Asegurar el registro de las actividades realizadas por el personal operativo, para su posterior revisión.

- Implementar los controles de seguridad definidos (software malicioso y accesos no autorizados).

- Definir e implementar procedimientos para la administración de medios informáticos de almacenamiento, como cintas, discos, casetes e informes impresos y para la eliminación segura de los mismos.

- Participar en el tratamiento de los incidentes de seguridad, de acuerdo a los procedimientos establecidos.

El Responsable de Seguridad de la información evaluarán los contratos y acuerdos con terceros para garantizar la incorporación de consideraciones relativas a la seguridad de la información involucrada en la gestión de los productos o servicios prestados.

Cada Propietario de la Información, junto con el Responsable de Seguridad de la Información determinará los requerimientos para resguardar la información por la cual es responsable.

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, revisará las actividades que no hayan sido posibles segregar. Asimismo, revisará los registros de actividades del personal operativo.

Control: Documentación de los Procedimientos

Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta Política y sus cambios serán autorizados por el Responsable de Seguridad de la Información.

Control: Cambios en las Operaciones

Se definirán procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio debe ser evaluado previamente en aspectos técnicos y de seguridad.

Control: Planificación de la Capacidad

El Responsable del Área Informática, o el personal que éste designe, efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuados.

Categoría: Protección contra el malware (código malicioso)

Proteger la integridad del software y la integración. Se requiere tomar precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no-autorizados. El software y los medios de procesamiento de la información son vulnerables a la introducción de códigos maliciosos; como ser, entre otros, virus Troyanos, bombas lógicas, etc.

Control: Resguardo de la Información

El Responsable del Área Informática, de Seguridad de la Información y los Propietarios de Información determinarán los requerimientos para resguardar cada software o dato en función de su criticidad. En base a ello, se definirá y documentará un esquema de resguardo de la información.

Control: Registro de eventos

Se producirán y mantendrán registros de auditoría en los cuales se registren las actividades, excepciones, y eventos de seguridad de la información de los usuarios, por un período acordado para permitir la detección e investigación de incidentes.

Control de Software Operacional

Garantizar la seguridad de los archivos del sistema.

Se debe controlar el acceso a los archivos del sistema y el código fuente del programa, y los proyectos TI. Asimismo, las actividades de soporte se debieran realizar de una manera segura.

Gestión del cambio de equipamiento y en las redes de comunicaciones

La gestión de cambios de red es un proceso que tiene la intención de reducir el riesgo de un cambio fallido. Este proceso implica varios pasos que aseguran cambios exitosos, pero ¿cómo funciona cada paso?

El proceso de gestión de cambios en el equipamiento y en la red de comunicaciones se basa en la aplicación de varios principios operativos básicos, como los siguientes:

- Determinación del alcance y análisis de riesgos
- Revisión por pares
- Pruebas y validación previas a la implementación

- Implementación y pruebas
- Actualizaciones de documentación.

Alcance y análisis de riesgos

Primer paso debe ser evaluar el alcance de un cambio propuesto. Determine qué servicios podrían verse afectados y quién los utiliza. El término radio de explosión se usa con frecuencia para describir el alcance del efecto que puede tener un cambio, incluidos los posibles resultados negativos.

Los equipos querrán medir el alcance en términos de los dos factores siguientes:

1. El número de puntos finales afectados por un cambio; y
2. La importancia de los servicios a los que podría afectar un cambio.

Revisión por pares

El siguiente paso es realizar una revisión por pares. Si bien los equipos pueden realizar este paso antes del análisis de riesgos, es mejor utilizar el nivel de riesgo para conducir la minuciosidad de una revisión por pares. Los cambios de rutina, como los cambios en la lista de control de acceso o la modificación de LAN virtuales, probablemente recibirán revisiones rápidas. Las pruebas automatizadas y el despliegue de cambios de rutina pueden ayudar a mitigar el riesgo de revisiones rápidas en pares.

El personal interno que está familiarizado con la red llevará a cabo la mayoría de las revisiones por pares. Sin embargo, si un cambio está fuera de lo normal, tiene sentido contar con un experto del proveedor del equipo para realizar la revisión. Las revisiones deben retroalimentar la fase de análisis de riesgos, potencialmente actualizando las mediciones técnicas de riesgo, como indicar si las pruebas y la documentación son suficientes.

Pruebas previas a la implementación y validación

La automatización de los cambios repetitivos de bajo riesgo puede eliminar la tentación de omitir las pruebas en los cambios que los equipos perciben como de bajo riesgo. Por supuesto, cuanto mayor es el alcance y el riesgo, más importante es probar y validar adecuadamente el cambio propuesto.

La prevalencia de instancias de SO de enrutador virtual y conmutador hace que sea más fácil automatizar la creación de topologías de red de prueba sin costosas inversiones en hardware. Para crear la topología de red virtual y derribarla cuando las pruebas se hayan completado con éxito.

Las pruebas previas a la implementación incluyen varios pasos que los equipos deben seguir para evaluar un cambio propuesto:

1. Verifique que la red de prueba funcione actualmente según lo previsto antes del cambio.

2. Implemente el cambio en una infraestructura de prueba Los equipos deben usar procesos automatizados para evitar errores humanos y reducir el tiempo para validar el cambio. Si la validación en el entorno de prueba falla, determine la razón. ¿Falló porque el cambio fue incorrecto o fue porque la red de prueba no representa con precisión la red real?

3. Pruebe el proceso de cambio de retroceso para que sea fácil volver al estado anterior si algo sale mal. El cambio de retroceso debería devolver la red al estado inicial, que los equipos pueden validar repitiendo el Paso 1.

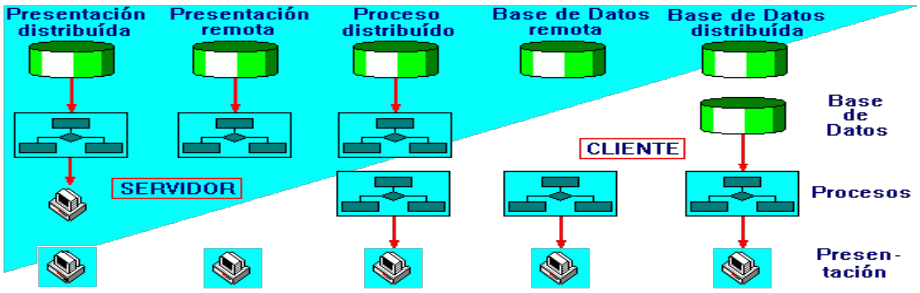
Implementación y prueba

La implementación y las pruebas posteriores a la implementación y el paso de validación deben seguir el mismo proceso que en los Pasos 1 y 2 de las pruebas previas a la implementación. Si los equipos han hecho un buen trabajo de pruebas y validación previas a la implementación, no debería ocurrir nada inesperado. Si las pruebas posteriores al cambio detectan un problema inesperado, los equipos deben retroceder el cambio y verificar la restauración del servicio.

Documentación y actualizaciones de gestión de red

Idealmente, los equipos crearán y actualizarán documentos durante el proceso de creación del cambio, permitiéndoles revisar la documentación y los cambios en la administración de la red junto con los detalles del cambio. Una vez que los equipos han implementado y verificado el cambio, pueden incorporar los cambios de documentación en el sistema de documentación de la red.

Planificación de la capacidad del centro de datos



Planificación de la capacidad del centro de datos bien hecha.

La vida útil de una instalación típica de centro de datos abarcará varias generaciones de equipos de TI. Por lo tanto, la planificación, o la falta de planificación, puede tener un gran impacto en la efectividad del diseño del centro de datos .

La planificación para futuras cargas, incluso en un nuevo centro de datos, es crítica. La capacidad de potencia y enfriamiento insuficiente para soportar estas cargas puede conducir a la pérdida de ingresos, a una reducción de la productividad y a una experiencia inaceptable para el cliente.

Creemos que un enfoque gradual y gradual para la planificación de la capacidad es el mejor. El primer paso es comprender los requisitos iniciales de energía de carga de TI (es decir, las necesidades de energía de los servidores, almacenamiento, dispositivos de red).

Luego se establece una estrategia de desarrollo incremental, basada en las expansiones esperadas de la carga de TI.

La metodología implica generar una cuidadosa estimación futura de la carga final de TI máxima y mínima posible. También se debe entender el tiempo de aceleración para alcanzar la carga final de TI. A partir de esta información, se puede estimar una carga estadísticamente «esperada». Tal enfoque considera tanto la capacidad de la infraestructura de energía requerida para suministrar energía a la carga como el volumen de enfriamiento requerido.

Beneficios de costos de planificación “escalonados”

El enfoque de introducción gradual permite que la capacidad de energía y enfriamiento crezca con la carga de TI, evitando el capital y los gastos operativos (incluidos el costo de energía y el mantenimiento) de los equipos que aún no se necesitan.
Al correlacionar los recursos de energía, enfriamiento y espacio con servidores individuales, estas herramientas proporcionan de manera proactiva una conciencia en tiempo real de la carga de TI y las capacidades de energía y enfriamiento restantes. En cada punto de su estrategia de crecimiento, existe la oportunidad de reevaluar si el crecimiento futuro aún es necesario.

Al escalar la capacidad a lo largo del tiempo en lugar de construir para la capacidad proyectada final por adelantado, vemos los siguientes beneficios:

Reducción de los costos de energía : la factura de electricidad es un poderoso incentivo para implementar las mejores prácticas de planificación de capacidad.
Cuando el costo de la energía era bajo, a menudo era una cuestión de orgullo y preparación tener un centro de datos con mucha energía de reserva y capacidad de

enfriamiento para «manejar cualquier cosa». Pero hoy, con un suministro de energía estresado y un costo en aumento, la capacidad excesiva aumenta tanto los gastos operativos como la huella de carbono.

Evitar la capacidad no utilizada : en la mayoría de los casos, un centro de datos nunca alcanzará la carga máxima para la que se planificó originalmente. Esto significa que el centro de datos pasará la totalidad de su vida soportando el exceso de capacidad costoso.

Un enfoque de introducción gradual mitiga este riesgo de instalar capacidad que deberá pagarse, pero que nunca se utilizará.

Reducción en el costo de mantenimiento: el equipo instalado debe mantenerse y repararse incluso si la capacidad no se utiliza. Al instalar solo lo que se necesita para soportar la carga actual, se pueden evitar gastos de servicio significativos: no hay gastos de servicio para el equipo que no tiene.

Como elaborar una política de resguardo

Una política de resguardo es una forma de organizar y priorizar la información a resguardar, se toman en cuenta estos puntos:

- ¿Que resguardar?: Que bases de datos se van a respaldar
- ¿Donde se resguardará?: En que unidad o la nube de almacenamiento se guardarán los archivos
- ¿Porque resguardar?: El porque del respaldar dichos archivos
- ¿Como resguardar?: El procedimiento a utilizar para el respaldo de los archivos
- ¿Que herramientas utilizar?: Que programas y herramientas se usarían para resguardar los archivos
- ¿Quien lo va a resguardar?: Es la persona que realizará los respaldos
- ¿Cuantas copias se realizarán?
- ¿De que tipo?
- Local: Si el resguardo se realizará en un dispositivo interno, como otro servidor
- Externo: Si se realiza en un servidor externo o en la nube

Cómo Manejar una Falla de Seguridad

Hay muchas maneras de mejorar la seguridad

Para hacer frente a un fallo de seguridad de forma rápida y eficiente, se deben tener claro, primero, algunos pasos básicos a tomar en caso de que tu sitio web se hackeado.

1. Comunícate con tu proveedor de web hosting: Una vez que notas un comportamiento sospechoso en tu página web, primero debes notificar a tu proveedor de web hosting y pedirles que comprueben si existen problemas potenciales. De esta manera, le permitirás a tu hosting asegurarse de que los datos de los otros usuarios no se vean afectados, especialmente si tu sitio web está alojado en un servidor compartido.

2. Baja tu sitio web: Cerrar tu sitio web impedirá a los usuarios acceder a sus cuentas y, potencialmente, revelar su información personal a los piratas informáticos. Además, también impedirás a los hackers continuar husmeando en los datos que están dentro del sitio.

3. Cambia todas las contraseñas: Tras el cierre de tu sitio web, deberás cambiar las contraseñas para todas las cuentas utilizadas para su gestión – FTP, cPanel, MySQL, etc.

4. Comprueba los registros de datos en busca de actividades inusuales: Examinando los registros de acceso más recientes, podrás ser capaz de determinar cómo se llevó a cabo el ataque y entender si tu sitio web es su objetivo real.

5. Repara el problemaSi ni tu equipo de trabajo ni tu proveedor de hosting es capaz de determinar la naturaleza del ataque, deberás buscar la ayuda de un experto en seguridad externa. Después de identificar la causa del ataque, podrás arreglar la vulnerabilidad y activar tú sitio web de nuevo.

6. Identificar posibles daños y notificar a los usuarios comprometidos: En cuanto identifiques los datos afectados, notifica a tus clientes sobre la violación y pídeles que cambien sus contraseñas. Asegúrate de sólo contactar a los usuarios que han sido afectados en lugar de enviar mensajes de correo electrónico a todo el mundo.

La presencia digital que cada empresa se esfuerza por lograr requiere de una estrategia para el manejo de las brechas de seguridad. En las empresas más pequeñas o las que acaban de comenzar la expansión de su base de usuarios, tales estrategias quedan pendientes.

Incluso estando alojados en servidores de buena reputación, la mayoría de los sitios web siguen siendo vulnerables a las violaciones, sobre todo porque los métodos de hacking se desarrollan para mantenerse vigentes. Por lo tanto, una estrategia detallada violación de la seguridad debe ser una parte del plan de marketing de cada empresa, ya que puede eventualmente llegar a ser la mejor manera de mantener a los clientes.

Si usted tiene alguna preocupación acerca de su tienda de comercio electrónico existente, póngase en contacto con nuestro amable equipo de soporte técnico a través de Live Chat o la unidad de soporte.

GESTION DE ACTIVOS

El Organismo debe tener un conocimiento preciso sobre los activos que posee como parte importante de la administración de riesgos. Algunos ejemplos de activos son:

- **Recursos de información**: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad y contingencia, información archivada, etc.

- **Recursos de software**: software de aplicaciones, sistemas operativos, herramientas de desarrollo y publicación de contenidos, utilitarios, etc.

- **Activos físicos**: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PABXs, máquinas de fax, contestadores automáticos, switches de datos, etc.), medios magnéticos (cintas, discos, dispositivos móviles de almacenamiento de datos —pen drives, discos externos, etc.—), otros equipos técnicos (relacionados con el suministro eléctrico, unidades de aire acondicionado, controles automatizados de acceso, etc.), mobiliario, lugares de emplazamiento, etc.

- **Servicios**: servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.).

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen

Generalmente, la información deja de ser sensible o crítica hasta cuando la información se ha hecho pública.

La información adopta muchas formas, tanto en los sistemas informáticos como fuera de ellos. Puede ser almacenada (en dichos sistemas o en medios portátiles), transmitida (a través de redes o entre sistemas) e impresa o escrita en papel. Cada una de estas formas debe contemplar todas las medidas necesarias para asegurar la confidencialidad,

integridad y disponibilidad de la información. Por último, la información puede pasar a ser obsoleta y por lo tanto, ser necesario eliminarla.

Objetivo

- Garantizar que los activos de información reciban un apropiado nivel de protección.
- Clasificar la información para señalar su sensibilidad y criticidad.
- Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

Alcance

Esta Política se aplica a toda la información administrada en el Organismo, cualquiera sea el soporte en que se encuentre. Responsabilidad

Los Propietarios de los Activos son los encargados de clasificarlos de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada

la clasificación efectuada, de definir las funciones que deben tener permisos de acceso a los activos y son responsables de mantener los controles adecuados para garantizar su seguridad.

El Responsable de Seguridad de la Información es el encargado de asegurar que información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

Cada Propietario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea cumplimentado de acuerdo a lo establecido en la presente Política.

Responsabilidad sobre los activos

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

Inventario de activos

Se identificarán los activos de información del Organismo. Existen muchos tipos de activos, que incluyen:

a) información: bases de datos, archivos de datos, documentación, contratos, acuerdos;

b) activos de software: software de aplicaciones, software de sistemas, herramientas de desarrollo, y utilitarios;

c) activos físicos: equipamiento de computación, equipamiento de comunicaciones, medios removibles y otros equipamientos;

d) instalaciones: edificios, ubicaciones físicas, tendido eléctrico, red de agua y gas, etc.;

e) servicios: servicios de cómputo y de comunicaciones, servicios generales, por ejemplo: calefacción, iluminación, energía, y aire acondicionado;

f) personas, y sus calificaciones, habilidades y experiencia;

g) activos intangibles, tales como la reputación y la imagen del Organismo

El encargado de elaborar el inventario y mantenerlo actualizado es cada Responsable de Unidad Organizativa.

Uso aceptable de los activos

Todos los empleados, contratistas y usuarios de terceras partes deben seguir las reglas para el uso aceptable de la información y los activos asociados con las instalaciones de procesamiento de la misma, incluyendo:

a) correo electrónico,

b) sistemas de gestión,

c) estaciones de trabajo,

d) dispositivos móviles,

e) herramientas y equipamiento de publicación de contenidos,

Clasificación de la información

Objetivo

Asegurar que la información reciba un nivel de protección apropiado.

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

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

Gestión de medios Objetivo

Evitar la divulgación no-autorizada; modificación, eliminación o destrucción de activos; y la interrupción de las actividades. Los medios se debieran controlar y proteger físicamente.

Se deben establecer los procedimientos de operación apropiados para proteger los documentos, medios de cómputo (por ejemplo, cintas y discos), entrada/salida de datos (input/output) y documentación del sistema de una divulgación no-autorizada, modificación, eliminación y destrucción.

Control: Administración de Medios Informáticos Removibles

El Responsable del Área Informática, con la asistencia del Responsable de Seguridad de la Información, implementará procedimientos para la administración de medios informáticos removibles, como cintas, discos, pen drives e informes impresos. El cumplimiento de los procedimientos se hará de acuerdo a la cláusula e deben considerar las siguientes acciones para la implementación de los procedimientos:

a) Eliminar de forma segura los contenidos, si ya no son requeridos, de cualquier medio reutilizable que ha de ser retirado o reutilizado por el Organismo.

b) Requerir autorización para retirar cualquier medio del Organismo y realizar un control de todos los retiros a fin de mantener un registro de auditoría.

c) Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores y la criticidad de la información almacenada.

MAGERIT – ISO - Recursos Humanos

Formalización de las actividades

Roles y funciones

- En el proceso de gestión de riesgos aparecen varios actores. Cuales son sus funciones y responsabilidades.

Órganos de gobierno

- En este epígrafe se incluyen aquellos que órganos colegiados o unipersonales que deciden la misión y los objetivos de la Organización.

- Típicamente se incluyen en esta categoría los altos cargos de los organismos. Cuando existe un Comité de Seguridad de la Información, suele aparecer en este nivel.

- Estos órganos tienen la autoridad última para aceptar los riesgos con que se opera. Se dice que son los “propietarios del riesgo”.

Dirección ejecutiva

- En este epígrafe se incluyen aquellos órganos colegiados o unipersonales que toman deci siones que concretan cómo alcanzar los objetivos de negocio marcados por los órganos de gobierno.

- Típicamente se incluyen en esta categoría los responsables de unidades de negocio, los responsables de la calidad de los servicios prestados por la organización, etc.

Dirección operacional

- En este epígrafe se incluyen aquellos órganos colegiados o unipersonales que toman deci siones prácticas para materializar las indicaciones dadas por los órganos ejecutivos.

- Típicamente se incluyen en esta categoría los responsables de operaciones, de producción, de explotación y similares.

Pirámide Jerárquica Típica

Esquema de Seguridad

En el Esquema de Seguridad de identifican ciertos roles que pueden verse involucrados en el proceso de gestión de riesgos:

Responsable de la información

Tiene la responsabilidad última sobre qué seguridad requiere una cierta información manejada por la Organización. A este nivel se suele concretar la responsabilidad sobre datos de carácter personal y sobre la clasificación de la información. A veces este role lo ejerce el Comité de Seguridad de la Información.

Responsable del servicio

Típicamente a nivel de gobierno, aunque a veces baja a nivel ejecutivo. Tiene la responsablidad última de determinar los niveles de servicio aceptables por la Organización. A veces este role lo asume el Comité de Seguridad de la Información.

Responsable de la seguridad

Típicamente a nivel ejecutivo, actuando como engranaje entre las directrices emanadas de los responsables de la información y los servicios, y el responsable del sistema. A su vez funciona como supervisor de la operación del sistema y vehículo de reporte al Comité de Seguridad de la Información.

En lo que respecta al proceso de gestión de riesgos, es la persona que traslada la valoración de los activos esenciales, que aprueba la declaración de aplicabilidad de salvaguardas, los procedimientos operativos, los riesgos residuales y los planes de

seguridad. En esta función, suele ser la persona encargada de elaborar los indicadores del esto de seguridad del sistema.

Responsable del sistema

A nivel operacional. Toma decisiones operativas: arquitectura del sistema, adquisiciones, instalaciones y operación del día a día. En lo que respecta al proceso de gestión de riesgos, es la persona que propone la arquitectura de seguridad, la declaración de aplicabilidad de salvaguardas, los procedimientos operativos y los planes de seguridad. También es la persona responsable de la implantación y correcta operación de las salvaguardas.

Administradores y operadores

Son las personas encargadas de ejecutar las acciones diarias de operación del sistema se aún las indicaciones recibidas de sus superiores jerárquicos.

Matriz RACI

La matriz que se expone a continuación es orientativa y cada organismo deberá adecuarla a su organización particular.

La matriz de la asignación de responsabilidades (RACI por las iniciales, en inglés, de los tipos de responsabilidad) se utiliza generalmente en la gestión de proyectos para relacionar actividades con recursos (individuos o equipos de trabajo). De esta manera se logra asegurar que cada una de las tareas esté asignada a un individuo o a un órgano colegiado.

Responsible: Este rol realiza el trabajo y es responsable por su realización. Lo más habitual es que exista sólo un R, si existe más de uno, entonces el trabajo debería ser subdividido a un nivel más bajo, usando para ello las matrices RASCI. Es quien debe ejecutar las tareas.

Accountable: Este rol se encarga de aprobar el trabajo finalizado y a partir de ese momento, se vuelve responsable por él. Sólo puede existir un A por cada tarea. Es quien debe asegurar que se ejecutan las tareas.

Consulted: Este rol posee alguna información o capacidad necesaria para terminar el trabajo. Se le informa y se le consulta información (comunicación bidireccional).

Informed: Este rol debe ser informado sobre el progreso y los resultados del trabajo. A diferencia del Consultado, la comunicación es unidireccional.

- niveles de seguridad requeridos por la información: A I R C

- niveles de seguridad requeridos por el servicio : I A R C
- análisis de riesgos I I A/R C
- declaración de aplicabilidad I I A/R C
- aceptación del riesgo residual I A A R I
- implantación de las medidas de seguridad I I C A R
- supervisión de las medidas de seguridad A C R

SO 27001 protege la información relativa a la gestión de los Recursos Humanos.

Selección y contratación de los empleados
Una persona puede incorporarse a una empresa por primera vez o cambiar de puesto dentro de la misma. Esto implica un acceso nuevo a información de carácter sensible para la empresa y, que si tiene implantada la norma ISO-27001 estará protegida.

Aun así es necesario plantear acciones preventivas para que un mal uso de la información no provoque riesgos de consecuencias indeseables. Cuando se va a contratar a una persona, la organización debería comprobar sus antecedentes, dentro de los márgenes de la legislación en privacidad y protección de datos, verificando el contenido de su currículum, las certificaciones académicas y profesionales.

En el contrato que se vaya a firmar deben estar plasmados las condiciones y términos sobre la responsabilidad en seguridad de la información a la que tendrá acceso el nuevo empleado, y que éste deberá aceptar. Estas cláusulas deben contener al menos:

- Responsabilidades sobre la propiedad intelectual y protección de datos.
- Obligación de confidencialidad y de no revelar ningún dato de la organización.
- Responsabilidades sobre el tratamiento de recursos y la clasificación de la información.

- Acciones a llevar a cabo en caso de incumplimiento de requisitos de seguridad y/o de la política.

- Responsabilidades con la información que reciba de otras compañías y la que se trata fuera de la organización.

Formación de empleados

Los empleados deben estar seguros de sus funciones y de las acciones que lleven a cabo en la empresa para no cometer errores que puedan afectar a la integridad de la información de la organización. Para que esto sea así deberán recibir la formación, educación, motivación y concienciación necesaria acerca de procedimientos de seguridad y el correcto uso de la información.

Estas obligaciones son responsabilidad de la organización que, según ISO27001 debe manifestar su liderazgo y compromiso en relación al Sistema de Gestión de la Seguridad de la Información.

Además de recibir esta formación, un empleado debe tener claro con quien debe ponerse en contacto en caso de requerir un asesoramiento de seguridad y qué procedimientos existen para identificar y gestionar incidencias de seguridad.

Cuando se genere una incidencia se aplicará el proceso disciplinario establecido previamente. Tendrán que ser medidas ajustadas a la gravedad de la infracción ocurrida y al entorno donde se produjo.

Finalización del trabajo o cambio de puesto

Desde el momento en que se decide que un empleado saldrá de la empresa hay que llevar a cabo una gestión de dicha salida. Esta gestión debe tratar la retirada de los privilegios y permisos de acceso, del material que estaba utilizando y de cualquier otro que tenga posesión.

Si lo que se produce es un cambio de puesto de trabajo dentro de la misma empresa, a este empleado se le deberán retirar los accesos que ya no le sean necesarios y cambiar cualquier contraseña de acceso a cuentas que ya tampoco vaya a necesitar.

En estos casos influyen aspectos como:

- Causa de finalización del puesto de trabajo.

- Responsabilidades del empleado.

- Valor de la información que manejaba.

Según el caso se podría hasta retirar los derechos de los que disfrutase el empleado un día antes de su salida, y si participara en grupos de trabajo, éstos deberían tenerlo en conocimiento para dejar de compartir información con él.