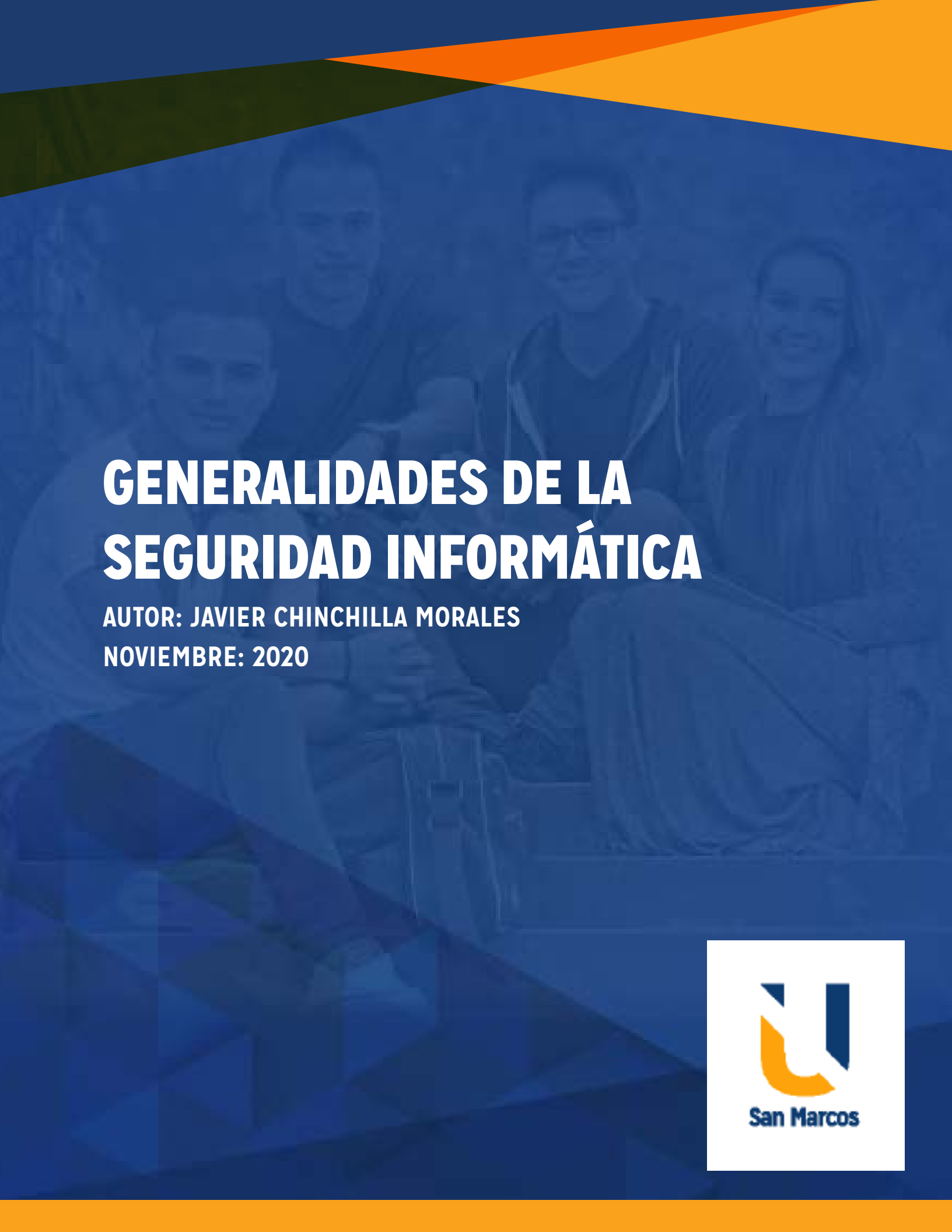

GENERALIDADES DE LA SEGURIDAD INFORMÁTICA

AUTOR: JAVIER CHINCHILLA MORALES

NOVIEMBRE: 2020

San Marcos

Introducción

Hay pequeñas y medianas empresas que piensan que nunca van a tener **problemas de seguridad informática**. Que eso sólo pasa a las grandes empresas, que son las que tienen más dinero y por tanto los ciberdelincuentes están más interesados en ellas.
Lo cierto es que esto no es más que un mito, ya que son precisamente las pymes quienes muchas veces presentan más problemas de seguridad informática.
La seguridad informática en las pymes va mucho más allá de tener antivirus instalados en los ordenadores. Hay que seguir una serie de protocolos y tener cierto criterio para controlar todas las posibles vías a través de las que puede quedar afectada la privacidad, seguridad e integridad de los datos de una pyme.
Esto afecta a:

- La información que almacenas en los ordenadores de la empresa.
- Los datos de redes sociales y programas en la nube que uses
- Tu software de gestión o cualquier otro programa empresarial que tengas instalado
- Tus servidores si los tienes
- El acceso a tus computadoras, por vía directa o remota
- Los dispositivos de almacenamiento que utilices (memorias USB, discos duros externos…).
- El comportamiento de los usuarios (empleados).
- Tu red informática y especialmente tu red Wifi.

En definitiva, hay toda una serie de aspectos en los que la seguridad informática está en juego. Y no siempre tienen que ver con la tecnología, también hay que mirar el factor humano. Muchos problemas de seguridad informática vienen como consecuencia de la falta de cultura digital de los empleados.

Tabla de contenido

Los dominios y regulaciones asociadas

Las mejores prácticas ITIL

ITIL es exitoso porque describe prácticas que permiten a las organizaciones obtener beneficios, retorno de la inversión, y un éxito sostenible y continuo. Algunas de las razones por las que las organizaciones adoptan ITIL son:

- Entregar valor a sus clientes a través de los servicios que presta
- Integrar la estrategia del servicio con la estrategia del negocio y las necesidades del cliente
- Supervisar, medir y optimizar los servicios de TI que ofrece y el desempeño como Proveedor de Servicios
- Gestionar el presupuesto y la inversión en TI
- Gestionar riesgos
- Gestionar conocimiento de manera formal
- Cambiar la cultura organizacional apoyando el logro del éxito sostenido
- Mejorar la interacción y relación con los clientes
- Coordina la entrega de bienes y servicios a través de una red de valor, optimizando y reduciendo costos

La estrategia del servicio (Service Strategy)

Diseña el plan de acción que permitirá desarrollar una estrategia en la Organización en cuanto a las Tecnologías de la Información. Desarrolla varias áreas; entre ellas se incluyen las siguientes: Estrategia general, competitividad y posicionamiento de mercado, tipos de proveedores de servicio, gestión del servicio como un factor estratégico, diseño organizacional y estratégico, procesos y actividades clave, gestión financiera, dossier de servicios, gestión de la demanda, y responsabilidades y responsabilidades clave en la estrategia de servicios.

El diseño de los servicios (Service Design)

Desarrollan los conceptos relativos al diseño de Servicios TI, como diseño de arquitecturas, procesos, políticas, documentación. Se adentra además en la Gestión de niveles de servicio, diseño para gestión de capacidad, continuidad en los servicios TI, gestión de proveedores, y responsabilidades clave en diseño de servicios.

La transición del servicio (Service Transition)

Definen los temas relacionados a la transición de servicios, es decir, los cambios que se han de producir en la prestación de servicios comunes (del trabajo diario) en las empresas. Aspectos tales como la gestión de la configuración y servicio de activos, la planificación de la transición y de apoyo, gestión y despliegue de los Servicios TI, Gestión del Cambio, Gestión del Conocimiento, y por último las responsabilidades y las funciones de las personas que participen en el Cambio o Transición de Servicios.

La operación del servicio (Service Operation)

Aca se exponen las mejores prácticas a poner en marcha para conseguir ofrecer un nivel de servicio de la Organización acorde a los requisitos y necesidades de los Clientes (establecimiento del SLA – Service Level Agreement o Acuerdo de Nivel de Servicio).

Los temas incluyen objetivos de productividad/beneficios, gestión de eventos, gestión de incidentes, caso de cumplimiento, gestión de activos, servicios de help desk, técnica y de gestión de las aplicaciones, así como las principales funciones y responsabilidades para el personal de servicios que llevan a cabo los procesos operativos.

La mejora continua del servicio (Continual Service Improvement - CSI)

Explica la necesidad de la mejora continua como fuente de desarrollo y crecimiento en el Nivel de Servicio de TI, tanto interno como con respecto al cliente.

De acuerdo con este concepto, las entidades han de estar en constante análisis de sus procesos de negocio, y poner en marcha actuaciones una vez detectadas las necesidades con respecto a las TI de manera que estas sean capaces de responder a los objetivos, la estrategia, la competitividad y la gestión de la estructura y organización de las organizaciones que dispongan de infraestructura TI. De esta manera se trata de estar al tanto de los cambios que se producen en el mercado y de las nuevas necesidades de este también en cuanto a las TI.

La gestión de la configuración (Configuration Management)

Para cualquier organización es importante disponer de información sobre su infraestructura TI, y mantenerla lo más actualizada posible. - - La información que este proceso ha de mantener actualizada tiene que ver con los elementos de configuración (CI) y sus relaciones en la infraestructura. Estos CI se componen de los siguientes elementos: Hardware, Software, Personas, Componentes de red y Líneas de negocio.

Los informes han de aportar, al menos, la siguiente información:

- Financiera y política del producto: valor y depreciación de los componentes; licencias; nivel de estandarización de la infraestructura.
- Evaluación de impacto: componentes afectados por el despliegue de nuevas actuaciones y cambios; componentes necesarios frente a desastres y contemplados en el plan de recuperación.
- Provisión de servicios y precio: configuraciones de TI necesarias para ofrecer servicio; componentes necesarios.

La gestión de la disponibilidad (Availability Management)

El objetivo principal de la Gestión de la Disponibilidad es ofrecer una base para la satisfacción del cliente. Es decir, todos los servicios deben estar a punto siempre con respecto a los SLAs y a la infraestructura TI que la empresa ofrece.

La Gestión de la Disponibilidad se encuentra localizada por tanto en medio de varios procesos internos de la empresa, en contacto directo con la Gestión de los Niveles de Servicio, la Gestión de Incidencias, la Gestión de Problemas, la Gestión de Configuraciones, la Gestión de Capacidad y la Gestión de la Continuidad del

Servicio. Esto supone ser la responsable de dar respuesta rápida para ofrecer soluciones, por lo que la medición, el seguimiento y la monitorización de procesos, unidas a las reuniones basadas en informes y el análisis de la información para proponer acciones que mejoren el Servicio son sus principales tareas asignadas.

Las actividades anteriormente relacionadas establecen por tanto una gran entrada y salida de documentación. Es por eso que se necesita establecer un proceso que ponga en marcha lo que será una Gestión de la Disponibilidad, donde las actividades a realizar estarán relacionadas con esta documentación, siendo las siguientes:

- Análisis de los acuerdos.
- Planificación.
- Continuidad del Servicio (Mantenimiento).
- Seguridad del Servicio.
- Seguimiento.

Para realizar una correcta Gestión de la Disponibilidad del Servicio, es necesario establecer unas pautas de trabajo que permitan a la Organización definir las necesidades del cliente para ofrecer un servicio que se ajuste a sus necesidades de disponibilidad. En este sentido se pueden encontrar tres fases: Planificación, Control y Monitorización.

La gestión de seguridad (Security Management)

El objetivo de la planificación es establecer un cronograma y definir unas responsabilidades para la ejecución del Plan de Seguridad y su mantenimiento. Debido a la complejidad que entraña ser un aspecto de gestión horizontal, es decir, que toca prácticamente el resto de procesos del servicio, es recomendable que exista un documento rector donde se determinen fundamentalmente las responsabilidades de llevar a cabo esta gestión, los recursos de los que tendrá que hacer uso y por supuesto una planificación basada en objetivos. Este documento es la Política de Seguridad, que debería incluir: Responsabilidades, Porqué de las medidas de Seguridad, Objetivos, Estructura organizativa, Coherencia con estrategia de Negocio, Seguridad de los activos y de la información.

Esta política debe estar en línea con los requerimientos del negocio y la estrategia de la organización, de manera que sirva de marco desde el que desarrollar procesos y procedimientos que se desplieguen por toda la infraestructura que apoya al Servicio TI, con el fin de garantizar las dimensiones de la información (Confidencialidad, Integridad, Disponibilidad y Legalidad).

Conclusiones y recomendaciones

ITIL es una metodología que nos va a ayudar a que las cosas se puedan hacer de una forma más eficiente, ya que lo que se propone es que se adopten ciertas métricas y procedimientos que otros proveedores de IT adoptaron y que gracias a ellas son catalogadas como mejores prácticas.

El hecho de adoptar mejores prácticas implica que no tengamos que descubrir el hilo negro y que si alguien sabe cómo hacer las cosas y explotar los recursos nos podemos apoyar en el para que nosotros también podamos hacerlo. E mayor objetivo es que todos lleguemos a un nivel de eficiencia que se traduzca en una buena prestación de servicios.

Referencias bibliográficas

- Carpentier, J. (2016). *La seguridad informática* en la PYME. Editorial ENI.
- Cañon, L. (2015). *Ataques Informáticos Ethical Hacking y conciencia de seguridad informática en niños. (Trabajo de Fin de Grado).* Universidad Piloto, Colombia.

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica