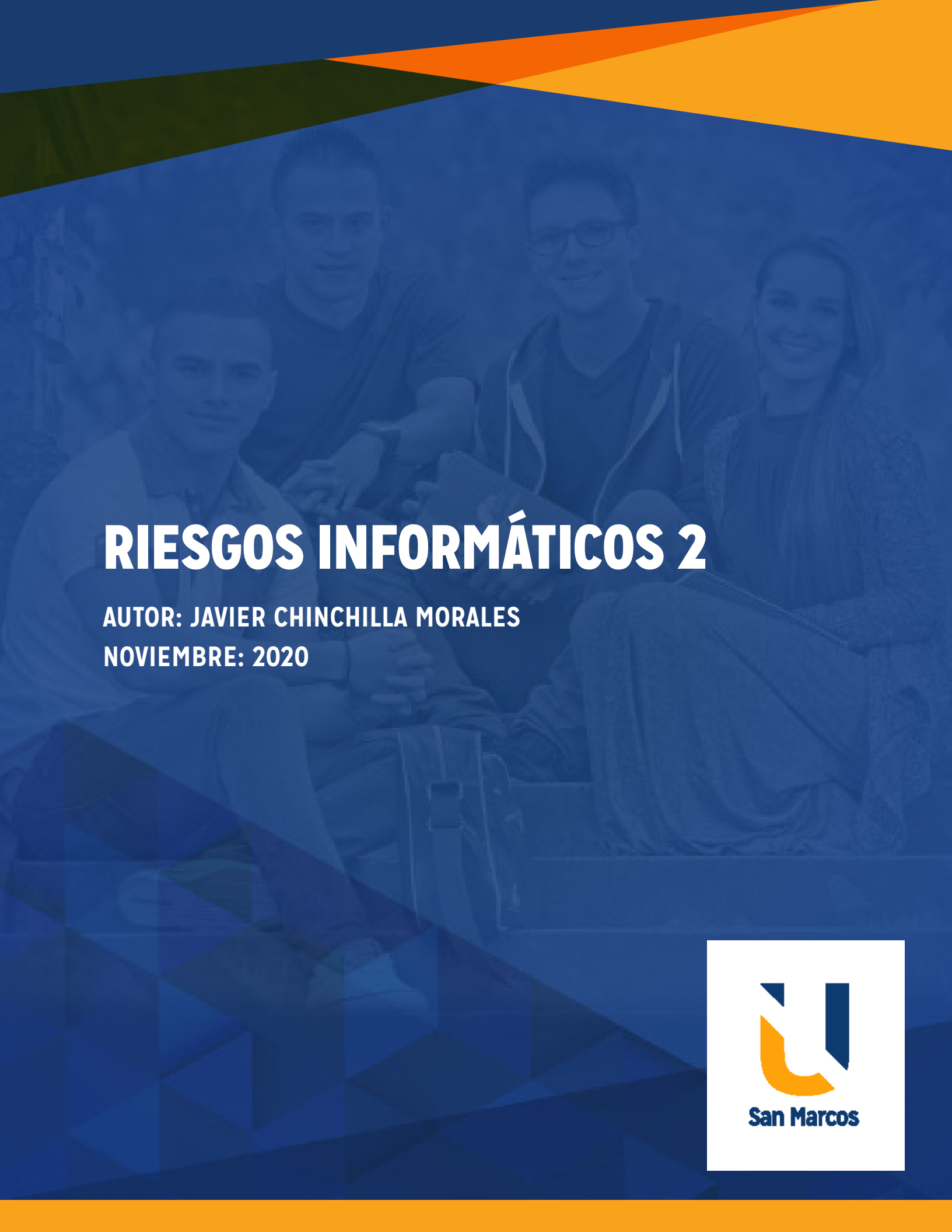

RIESGOS INFORMÁTICOS 2

AUTOR: JAVIER CHINCHILLA MORALES

NOVIEMBRE: 2020

San Marcos

Introducción

Las políticas de seguridad informática han surgido como una herramienta en las empresas para concienciar a los usuarios sobre la importancia y la sensibilidad de la información y de los servicios de la empresa.
Una política de seguridad es la forma de comunicación con los usuarios, estableciendo un canal de actuación en relación con los recursos y los servicios informáticos de la empresa. Describe lo que se desea proteger y el porqué,
meidante normas, reglamentos y protocolos a seguir, definiendo funciones y responsabilidades de los componentes de la organización y controlando el correcto funcionamiento.

Tabla de contenido

La política de seguridad

Los principios

Exite un campo muy amplio que dá inicios a ésta práctica como lo son:

- La confidencialidad o privacidad que debe impedir que personas no deseadas accedan al sistema, ni a la información disponible. Par eso es muy importante disponer de las herramientas oportunas para el control de accesos a los Sistemas y que la información confidencial sea cifrada.
- La integridad de la información a la que se tiene acceso, impidiendo que la información sea mnipulada por personal ajeno. Debe ser incluido en este punto además, la posible modificación de la información por causas accidentals en el desarrollo de los procesos.
- La disponibilidad de la información a cualquier usuario en cualquier momento y el sistema debe de ser capaz de recuperarse anto posibles fallos.

Estas políticas han surgido como una herramienta en las empresas para cocientizar a los usuarios sobre la importancia y la sensibilidad de la información y de los servicios de la empresa.

La elaboración del documento

En la creación de la política se debe considerar incluir los siguientes aspectos:

- El alcance de la politica, cubriendo todos los aspectos relacionados con la misma.
- Los objetivos y la descripción de los elementos involucrados, proteginedo todos los niveles: físico, humano, lógico y por supuesto logístico.
- Responsabilidades de los servicios y Recursos informáticos implicados.
- Los Requerimientos mínimos de Seguridad, incluyendo la estrategia a seguir en caso de fallo.
- Definición de las violaciones y las sanciones.
- Responsabilidades de los usuarios y sus accesos.

Dicha elaboración debe utilizar un lenguaje sencillo que pueda se entendido por todo el personal, se debe actualizar periódicamente, y para que surta efecto dentro de la organización la política debe ser aceptada y para ello debe de integrarse en el modelo de Negocio de la empresa para que el personal entienda de su importancia.

Las herramientas asociadas

Las herramientas mas recomedadas para la Seguridad informática son:

- El antivirus: estos aportan medidas de protección efectivas ante la deteccion de un malware o de otros elementos maliciosos, cierran posibles amenazas y son capaces de poner el dispositivo en cuarentena para evitar males mayores.
- El firewall: éste se dedica a escanear los paquetes de red y los bloquea o no según las reglas que previamente ha definido el administrador, pueden inspeccionar todo el tráfico de la web, identificar usuarios, bloquear accesos no autorizados y muchas mas acciones.
- El servidor proxy: es un dispositivo que actúa como intermediario entre enternet y las conexiones del navegador, filtra los paquetes que circulan entre ambos puntos.
- End Point Disk Encryption: tambien llamado como cifrado de punto final, es un proceso de codificación de datos para que nadie que no guarde la clave de descifrado pueda leerlo. Protégé los Sistemas operativos de la instalación de archivos corruptos, al bloquer los archivos almacenados en ordenadores, servidores y otros puntos finales.

- Escáner de vulnerabilidad: es una herramienta fundamental para todo tipo de empresas sin importer el tamaño o el ssector, el mismo detecta, analiza y gestiona los puntos débiles que tenga el sistema.

Los principales ejes de la estrategia de seguridad

El diagnóstico y la evaluación de las necesidades

El tratamiento de amenazas y vulnerabilidades cibernéticas comienza en el diagnóstico y análisis de los riesgos informáticos y para ello se debe establecer un plan para la gestión de vulnerabilidades de la empresa. Para conocer donde se encuentra la empresa con respecto a los riesgos informáticos se deben de llevar a cabo una serie de tareas como:

- Identificación o inventario de activos sensibles de vulnerabilidades y amenazas.
- Vulnerabilidades y amenazas communes a las que se expone la compañía.
- Cálculo de probabilidades en la que estas últimas puedan atacar los activos.
- Posibles impactos de las mismas sobre las operaciones.

El objetivo de todo este proceso se orienta a establecer estrategias adecuadas para mitigar los riesgos informáticos, el cual sigue siendo una de las principales preocupaciones de las empresas en materia de seguridad digital. Para el dianostico debemos evaluar los siguientes 5 aspectos:

- Seguridad digital de cara a la gestión de vulnerabilidades.
- Concentración de servicios de Seguridad vs desarrollo de equipos de Seguridad digital.
- Pros y contras de la contratación de servicios externos para mitigar los riesgos informáticos.
- Período de diagnóstico y evaluación de riesgos informáticos.
- Misceláneo de actividades posteriores al proceso de diagnóstico de riesgos informáticos.

Los planes operativos de Seguridad

Un plan de seguridad informática te permite entender donde puedes tener vulnerabilidades en tus sistemas informáticos, para una vez detectadas, tomar las medidas necesarias para prevenir esos problemas. No necesitas que tu plan de seguridad informática sea un documento demasiado extenso que cubra cualquier tipo de seguridad imaginable. Debe ser capaz de ayudar a proteger los datos y los sistemas críticos de tu negocio, asegurándote además que se ajuste a la legislación vigente y a la Ley de Protección de Datos. Tu plan de seguridad debe de tener varios pasos que debes dejar por escrito, los cuales se muestran a continuación:

- Identificación de lo que debemos proteger.
- Evaluación de riesgos: establecer qué es lo que podría poner en peligro los primeros activos.
- Priorización de la protección de TI: se debe decider qué amenazas son las más importantes e interesantes para empezar a proteger.
- Toma las precauciones adecuadas: se debe seleccionar cuales son los pasos que se deben de tomar para protegerse contra los riesgos que se han identificado

El acceso a los sistemas y los datos

Pensar en Seguridad de acceso a los sistema y a los datos es construír defensas desde el principio ya que es de vital importancia, para ello se deben diseñar, implementar y probar los Sistemas completes y seguros.
Si en la red ocurren acciones de aspecto sospechoso, como alguien o algo que intenta entrar, la detección de intrusos se activará. Los sistemas de detección de intrusos de red (NIDS) supervisan de forma continua y

pasiva el tráfico de la red en busca de un comportamiento que parezca ilícito o anómalo y lo marcan para su revisión. Los NIDS no sólo bloquean ese tráfico, sino que también recopilan información sobre él y alertan a los administradores de red.

La protección física

La definición nos habla del proceso por el cual aplicamos una serie de barreras de tipo físico, así como unos procedimientos determinados que nos permiten proteger nuestros recursos. Se trata de proteger, de colocar contramedidas y sistemas de prevención para que la información confidencial que exista en nuestro negocio siempre esté a buen recaudo. Esta protección se instalará alrededor de los equipos informáticos para que el acceso a los mismos no sea sencillo y que todo dispositivo tecnológico en la empresa esté protegido. ¿Pero para qué elementos nocivos nos estamos protegiendo? ¿qué es aquello que podemos considerar como una amenaza física para los sistemas informáticos de una empresa?

Las misma puede ser de tipo hostil como el robo, copia de información, sabotaje, suciedad que se dan por medio de agujeros y errores en la Seguridad física.

La protección lógica

Es un conjunto de procesos que nos ayudan a garantizar la Seguridad en los Sistemas y los programas destinados a gestionar datos y procesos, lo cual también hace referecia al acceso autorizado y ordenado de los usuarios a la información almacenada en la empresa, la misma sirve para garantizar que los programas, archivos y datos cuenten con procedimientos de protección correctos y seguros retringiendo el acceso a archivos y programas por parte de usuarios sin autorización.

Identificación y trazabilidad

La trazabilidad es un termino que es utilizado para el control de los procesos o la localización e identificación de los procesos correctos dentro del ámbito de desempeño de la empresa sobre todo es de mucha importancia llevarla deacuerdo a la información que se intercambia, cuales canals de comunicaciones se van a utilizar y dónde va a llegar. Con la trazabilidad garantizamos algunas ventajas como son: para la empresa el aumento de la Seguridad y beneficios económicos, para el cliente un aumento de confianza y para la administración una mayor eficacia en la gestión de incidencias.

La garantía de la disponibilidad del sistema de información

La disponibilidad es uno de los objetivos principales de la Seguridad en informática, y la misma se define como la capacidad de garantizar que tanto los Sistemas como los datos van a estar disponibles al usuario en todo momento, también supone que la información pueda ser recuperada en el momento en que se necesite, evitando cualquier tipo de pérdida o bloqueo, mateniéndolos a salvo de interrupciones previstas (que es cuando paralizamos nuestros Sistemas para realizar cambios, o mejoras) o interrupciones imprevistas (como un apagón, un error de hardware o software, un desastre natural, virus, accidents, o caídas involuntarias del sistema)

La sensibilización de los usuarios a la seguridad

La falta de sensibilización de los usuario ha hecho que el número de ataques no disminuya, esto según resultados de estudios actuales donde se indica que el 80% de los ataques a las organizaciones la entrada a los Sistemas es por medio de los usuarios, lo cual nos lleva a desarrollar empleados conscientes, capaces de

seguir las mejores practicas para proteger los Sistemas, haciendoles saber que el factor humano representa el recurso más valioso de la empresa. El sensibilizar a los usuarios es simplemente garantizar que cada miembro de la organización reciba la formación necesaria para protegerse a sí mismo y a la empresa de cualquier posible ataque.

Conclusiones y recomendaciones

La implementación de políticas de seguridad informática en una organización es una solución integral que no sólo busca proteger, preservar, administrar de una manera eficiente todo tipo de recursos con los que cuenta una organización, sino que también busca dar solución, prevenir, evitar, controlar y minimizar los daños de incidentes que afectan a la organización, por esto, preparar y capacitar al personal en temas asociados a la seguridad informática y cómo hacer frente a incidentes que se llegarán a presentar con el fin de responder de una manera adecuada es una de las principales metas de esta estrategia.

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