INTRODUCCION

La seguridad de la información es considerada como un conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma, en donde su manejo está basado en la tecnología y es necesario saber que puede ser confidencial, estar centralizada y tener un alto valor. Por lo tanto el trabajo se trazó como propósito determinar la estrategia que debe seguir la compañía «Viajes SIS» para fortalecer e implementar los controles que le permitan mitigar riesgos asociados a fuga de información, fraudes, deterioro de la imagen corporativa, Phishing, con el fin asegurar y proteger los procesos de la empresa. Para ello se desarrolla una metodología de corte analítico, apoyado en observaciones personales en la empresa, la entrevista de funcionarios y la información procedente de fuentes bibliográficas.

 Conocer y robustecer los controles existentes, para mitigar la materialización de riesgos como fraudes internos, teniendo en cuenta los datos estadísticos presentados para el 2015 y 2016. Disminuir los casos de fraudes internos y externos y así reducir las pérdidas económicas.

Existen falencias en la valoración de riesgos de seguridad de TODOS los activos de

Dificultad para el control y clasificación de los activos de información. No se encuentran establecidas en su totalidad, las políticas de seguridad con el fin de ir alineada con las estrategias y objetivos del negocio. Debido a que el área de seguridad de la información se encuentra terecerizada, no existe un control adecuado sobre los sistemas internos de la compañía.

Tipo de Investigación

« En su fase de elaboración del marco de referencia teórica y conceptual, el estudio es documental, que »consiste en un análisis de la información escrita sobre un determinado tema«1. En este caso, el de los aspectos organizacionales la compañía denominada »Viajes SIS« y las características del desarrollo de la norma ISO 27000.

Fuentes para la Obtención de Información

Como fuentes secundarias se emplearán bases documentales como tesis, artículos de revista, pdf, libros y consultas en la Web sobre la norma ISO 27000 y agencias de viajes.

Decreto 1820 de 2015. Decreto 166 de 2015. Resolución 148 de 2015.

Decreto 2183 de 11 de noviembre de 2015 «Por el cual se modifica el parágrafo 1 ° del artículo 2.2.4.2.7.4 de la Sección 7 del Capítulo 2 del.

La OTA argentina fue la única de las cinco agencias que más tiquetes internacionales venden en Colombia en aumentar sus ventas en los cinco primeros meses de 2015 respecto al mismo periodo de 2014, pues tanto los grupos de L'alianxa, Travel Group y Over obtuvieron descensos cercanos todos ellos al 5 por ciento. La cuota de mercado en las cinco mayores agencias de viajes del país se redujo levemente en estos primeros cinco meses del año, acaparando Aviatur la mayor caída, al pasar de representar en las mismas fechas del pasado 2014 casi un 17 por ciento de todas las ventas aéreas internacionales a través del BSP al 15.33 por ciento, mientras ni Despegar. Para el año 2016 Colombia superará fácilmente los US$5.000 millones en ingresos por concepto de turismo. Para las agencias de viajes, el 2016 mostró un horizonte positivo.

Otro aspecto evaluado en la encuentra realizada por la ANATO, es el porcentaje estimado de crecimiento y disminución de ventas durante la temporada para lo que se evidencio que el 63% de las agencias encuestadas determinaron que sus ventas aumentaron en promedio un 20. El 37% de las agencias encuestadas determinaron que sus ventas disminuyeron en promedio un 26.2% durante la temporada de Semana Santa 2016 con respecto al año 20154.

Al igual que en la Temporada anterior, los paquetes turísticos perdieron 4.4 puntos porcentuales frente a la encuesta del Temporada de Semana Santa 2015. La venta de tiquetes aéreos se constituye como el principal servicio de venta de las AGV con un 46% de participación, un año atrás, la venta de tiquetes internacionales representaba casi el 21% pero para el 2016, tan solo el 17%5.

Mayo 17 de 2014 «Los delincuentes usaban tarjetas clonadas para comprar tiquetes aéreos y vendérselos a los viajeros»

« Usando el nombre de reconocidas agencias de viajes, los delincuentes compraban tiquetes aéreos con tarjetas clonadas y los daban a los turistas que al llegar al aeropuerto descubrían que eran falsos. Antioquia» «la Asociación Colombiana de Agencias de Viajes y Turismo informó que ante la alta posibilidad de fraude que hay por agencias de viajes falsas, las cuales se incrementan cerca de 30 por ciento en diciembre, la Asociación lanzó una campaña para que los viajeros aprendan a identificar agencias legítimas así como los recursos, normas y decretos que comprometen y regulan al prestador de servicios.»En los últimos tiempos hemos recibido quejas de muchos usuarios que al momento de llegar al aeropuerto para viajar se enteran de que los documentos que llevan no son válidos«, dijo Raigosa. Añadió, que una de las principales acciones que hacen las agencias fraudulentas es pedir abonos anticipados de manera periódica y el cliente no se percata de pedir un recibo de caja oficial de esos depósitos. Al igual que preocupa la posibilidad de fraude, también lo hace la falta de denuncias de las personas ya que, según la entidad, el 50 por ciento de los usuarios no lo hace»7.

La Dijín, a través de un comunicado, informó que «no se han reportado casos en Colombia denunciados oficialmente, pero se cree que han sido afectadas algunas instituciones de gobierno y la banca». Allí, el texto nombra como posible afectado al Instituto Nacional de Salud. La Policía y el MinTIC le solicitó a las entidades del Estado realizar la revisión de sus plataformas Microsoft y actualizar los
http://www.eltiempo.com/colombia/medellin/alerta-por-1-000-posibles-agencias-de-viajes-falsas-41700 sistemas operativos de sus estaciones de trabajo y servidores, con el fin de mantenerlos al día en lo que se denomina 'parches' críticos y de seguridad.

Análisis de riesgos informáticos

Guía la selección de medidas de protección de costo adecuado.

Vulnerabilidades

Análisis consiste en la identificación de estas ausencias o debilidades. La mejor forma de llevarlo a cabo es a través de entrevistas individuales estructuradas con quienes tienen la responsabilidad de implementar las políticas institucionales mediante medidas administrativas o medidas de control. Se deben analizar los mecanismos que están presentes desde el punto de vista de cada una de las componentes de los activos, precisando que conceptos se emplearon para proponer un mecanismo para proteger un activo dado.

Enfocado a determinar valores numéricos a los componentes objeto del análisis, así como al nivel de posibles

Es sencillo mostrar el costo-beneficio en términos comprensibles a la alta dirección .

No requiere determinar valores numéricos a los componentes objeto del análisis, así coma al nivel de posibles

Los resultados son subjetivos, No hay una base para demostrar el costo-beneficio. La calidad del análisis depende del equipo conformado 14 .

Análisis de vulnerabilidad . Análisis del impacto estimado a la organización . Seguridad de la información. Redes, informática y sistemas de información .

Análisis del beneficio logrado con el costo estimado .

Requerimientos modernos sobre los modelos de control de acceso

En la medida que solo se requería vigilar las propiedades de seguridad de la información contenida en una sola computadora central, los modelos que se han estudiado hasta ahora eran suficientes. La información, los programas y los datos están dispersos en un número indeterminado de computadoras heterogéneas. No es posible basar el control en un monitor de referencia clásico, y la matriz de estado de seguridad es un concepto que tampoco se puede aplicar directamente. Se ha desarrollado la tecnología de la administración de identidades para resolver este problema.

Arquitecturas funcionales

La administración de identidades y de autorizaciones se puede llevar a cabo de dos maneras genéricas distintas. La secuencia necesaria para que sea posible esta administración consiste en que el usuario indique que desea hacer, que se le soliciten datos de identidad y autenticación verificables, y si mediante el servidor de identidades se acepta la autenticación, se consulte al servidor de autorizaciones para verificar sus derechos.

La administración de la identidad tiene un ciclo de vida

Administración delegada. Administración de contraseñas y sincronización.

Administración de contraseñas y la sincronización

La ayuda de administración de contraseñas puede resolver estos problemas. Esto quizás sea manejado par un servicio especializado que asegure la administración de la contraseña de un usuario para mantener un nombre común y una contraseña a través de sistemas dispares. Esto no crea necesariamente un acervo central de información de identidad para el uso por otras aplicaciones, pero puede conducir a eso.

Este modelo es el más aceptado en el servicio de autorizaciones. El concepto principal es que los usuarios gozan de acceso discrecional a los objetos del sistema. Esto simplifica la administración de los permisos y ofrece más flexibilidad para especificar y vigilar la obediencia de las políticas de protección. Los usuarios pueden registrarse en un perfil dado según sus responsabilidades y capacidades, y se les puede reasignar de un perfil a otro sin modificar la estructura de control de acceso.

Organización y no el usuario, pero en entornos civiles jerarquización puede ser inconveniente, o hasta imposible.

Así, surgen estándares sobre como almacenar la información en dispositivos portátiles, como diskettes y cartuchos de cinta, las especificaciones eléctricas de los módems y el protocolo necesario para que un programa cliente solicite una página de Web19.

El Gobierno sugiere a las entidades o empresas que tengan equipos utilizando

Los equipos con Windows 7 en adelante deben actualizarse. Las autoridades recomiendan nunca compartir información personal ni financiera solicitada a través de correos electrónicos, llamadas, mensajes de texto o redes sociales8«. Telefónica sufre ataque cibernético en su red corporativa»El gigante de las telecomunicaciones español Telefónica fue víctima el viernes de un incidente de ciberseguridad en su red corporativa que lo obligó a apagar todos los computadores de su sede en Madrid como medida preventiva, señaló una fuente de la compañía. « Estamos esperando a ver qué implicaciones tiene», declaró a la AFP una fuente de Telefónica que no quiso ser identificada.

Varios medios españoles informaron el viernes a última hora de la mañana que

Telefónica había sido víctima de un pirateo masivo hasta el punto de que sus empleados habían sido avisados por megáfono de apagar con urgencia los dispositivos.

De acuerdo con la entidad, «el ransomware, una variante de WannaCry, infecta la máquina cifrando todos sus archivos y utilizando una vulnerabilidad que puede infectar al resto de sistemas Windows conectados en esa misma red que no estén debidamente actualizados». Voceros de Telefónica han explicado que en varios de los equipos afectados, en la pantalla se pedía en pago de una cantidad en bitcoins. Igualmente han asegurado que mientras los equipos han estado apagados, los trabajadores han seguido desempeñando sus funciones, recurriendo a dispositivos móviles«. » En un comunicado, el Ministerio de Energía, Turismo y Agenda Digital señaló que el ataque sólo afecta puntualmente a equipos informáticos de trabajadores de varias empresas, entre ellas Telefónica, y que está trabajando con las compañías afectadas para solucionar cuanto antes la incidencia.

Así mismo, aseguró que el ataque «no compromete la seguridad de los datos ni se trata de una fuga» de los mismos.

Nacional para la Protección de las Infraestructuras Críticas del Ministerio del

En su alerta para empresas, el Incibe dijo que dispone de un servicio gratuito de análisis y descifrado de ficheros afectados por ciertos tipos de 'ransomware', denominado 'Servicio Antiransomware'.

La organización denominada «Viajes SIS» inicio como agencia de viajes en

Colombia en el año 2006, es una compañía nacional filial, incorporada a la asociación Internacional de Transporte Aéreo IATA. Cuenta con 200 empleados en Colombia, donde más de 94 son ejecutivos de ventas. Cuenta con un departamento corporativo especializado en viajes de negocios, además, con un área de planificación y organización de viajes de incentivos y congresos, tanto en Colombia como en el extranjero. Se ha destacado en el mercado de viajes por su perfil innovador y su preocupación constante por entregar un excelente servicio, que logra equilibrar calidad, precio y formas de pago.

Policita de sostenibilidad

La compañía «viajes» declara su compromiso con la implementación del Sistema de Gestión

para la Sostenibilidad, promoviendo la protección de los destinos turísticos nacionales, el patrimonio natural, cultural de la nación y el medio ambiente.

3 MARCO TEÓRICO

Administración de la seguridad. Todas las disciplinas de seguridad trabajan en forma conjunta para establecer una infraestructura de seguridad 1ue sirva a toda la organización.

Algunas políticas necesarias

Especifica cómo deben establecerse jerarquías de confidencialidad e integridad, y como se implementa su protección. Debe ponerse especial atención a la divulgación y destrucción de la información. También quien debe tener acceso a ser usuario del cortafuegos y quien puede tener información acerca de la configuración del mismo. Contienen procedimientos de auditoria del uso de este tipo de cuentas, particularmente sobre los procedimientos de identificación y autenticación, y su uso.

Determina en qué condiciones se debe cancelar el acceso privilegiado. Son particularmente importantes para organizaciones que tienen una diversidad de equipos de soporte técnico, y para aquellos que no están protegidos por un cortafuegos.

Normalmente confiamos en que la organización que nos vende el software no comete ningún Fraude, como cuando instalamos Windows. Este es el motivo por el que muchos consideran que el código Libre merece más confianza que et código propietario. Como contrapartida, ha habido intentos de contaminar código libre, como uno reciente que buscaba acudir una puerta trasera a la kernel de Linux.

Las politicas corporativas se encuentran vigentes.

Las amenazas se pueden clasificar en tres grandes grupos

Amenazas Terciarias o directas, que son Las que amenazan directamente el cumplimiento de nuestras expectativas. Amenazas Primarias, que son Las que evitan que se mantengan o lleguen a establecerse Las medidas que mitigan Las amenazas terciarias o secundaria. En la literatura de seguridad se presta una enorme atención a las amenazas terciarias.

Amenazas Terciarias

Los ataques tienen siempre detrás a un actor con una determinada motivación, medios y capacidad. Los errores pueden ser naturales, pero también se pueden manipular, como puede ser un cracker que genera un coredump en un sistema que este atacando.

Ataques

Conocer los posibles recursos y oportunidades de que dispone el atacante nos permitiría estimar que recursos se dedicaban a un ataque21. Los ataques descritos a continuación pueden suceder individualmente, o utilizarse en conjunto para producir el electo deseado por un atacante. El espionaje consiste en el acceso ilegitimo sea físico o lógico, a La información mensajes y servicios de La organización.

Escuchas

Los equipos de entrada/salida emiten radiaciones electromagnéticas que pueden ser interceptadas por sistemas como TEMPEST.

Lectura o Copia de Información

La Lectura o copia consiste en el acceso directo a La información, sin utilizar servicios ni sesiones autorizados.

La

Asegurarnos de que solo se puede acceder a información confidencial mediante sesiones autorizadas.

Los sistemas que tengan salida a Internet deben tener Filtros adecuados para evitar accesos no autorizados.

Lectura de mensajes o información cifrados

EL criptoanálisis consiste en el análisis de datos cifrados en bruto, sin que necesariamente conózcanos el algoritmo de cifrado ni nada acerca de que información puede contenerse en Los datos. Es curiosa La pobre barrera que supone codificar por sustitución, utilizando un símbolo para significar otro, supone para el criptoanálisis , dada que la informaciones por naturaleza muy ordenada, lo que resulta sencillo comprobar sin necesidad de tener una comprensión de La información.

Esto es lo que hace una compañía de tarjetas de crédito que le pide información personal por teléfono ante una compra importante y fuera de lo habitual.

Sabotaje

La protección más efectiva ante esta amenaza es la eliminación de oportunidades, y el uso de medidas de reducción del impacto.

La interrupción de un mensaje o un servicio, o el borrado de información es auto-explicativa.

Modificación y Generación malintencionada de datos o información

Modificar o generar datos se puede hacer sobre el almacenamiento o en la transmisión de datos. La diferencia entre generar o modificar datos intencionadamente es que simplemente puede deteriorar La calidad de nuestra información, mientras que generar modificar información es una Forma más avanzada de ataque que en la comunidad de inteligencia se conoce coma desinformación.

Ante esta amenaza debemos tomar las mismas medidas que ante cualquier otro atacante externo.

El usuario y contraseña son realizar la Comparación con los

Se nos concede acceso.

Lo cual nos conduce a Los posibles problemas

Podemos olvidar La contraseña. Alguien puede ver como la tecleamos o espiar tolo que tecleamos indirectamente. Un tipo de programas llamados keytoggers que graba todo lo que tecleamos en un archivo, de modo que puede leerse La contraseña posteriormente. EL sistema en que tecleamos puede transmitirla subrepticiamente a un tercero24.

La mayor parte del código malicioso se aprovecha de una característica

Tanto Los ataques a la pila como al «Formal string» sustituyen datos como direcciones como instrucciones por información de usuario, que adquiere un control del sistema fuera del control de Los controles de accesos. EL código malicioso se aprovecha también de Los sistemas operativos que confían en todo software el que tienen acceso, en lugar de confiar sato en software explícitamente autorizado. No olvidemos que un antivirus, en et rondo, es un parche para un defecto común a casi todos Los sistemas operativos modernos. La única garantía de que el software que instalamos en nuestros sistemas no tiene ningún comportamiento distinto del que hemos contratado es disponer del código fuente.

En segundo lugar, se encuentran los casos en los cuales no se adjunta el visto bueno correspondiente para poder atender la solicitud, para este ítem se encuentran las excepciones de permisos que deben contar con un visto bueno por parte de gestión humana cuando esta supera los 30 días, usuarios para los aprendices Sena y practicantes universitarios, ya que este debe contar con el visto bueno del jefe directo, Gráfico 7.

Se evidencia incumplimiento en los controles de monitoreo de acceso de usuarios ya que en el procedimiento se encuentra definido que para las aplicaciones de alta criticidad se debe realizar cada 2 meses y para las apelaciones de baja criticidad cada 3 meses.

Planes de acción

ID Management, se denomina como un sistema integrado de políticas y procesos organizacionales que pretende facilitar y controlar el acceso a los sistemas de información.

Seguridad móvil

Oracle Mobile Security Suite proporciona una solución de gestión de movilidad empresarial integral que aborda una combinación de modelos BYOD y pertenecientes a la compañía sin comprometer la seguridad, la experiencia de los usuarios o la privacidad.

Se debe ajustar las normas de buen uso de información dado que el inventario se actualiza anualmente. Numeral 17.

No se encuentra la aprobación de seguridad de la información en los planes de contingencia definidos. Tabla 5.

Escalas de calificación ISO 27001

Para cada una de estas escalas se define un porcentaje de acuerdo a la siguiente tabla, con el fin de obtener el cumplimiento.

También fue posible identificar que no tienen claro lo que es una política de seguridad de la información, ya que conocen que no deben prestar los usuarios de acceso a las aplicaciones, porque se encuentra prohibido, o que no deben dejar impresa información de los clientes en los puestos de trabajo, pero no identifican que estas son políticas de seguridad de la información. Este requisito obtuvo una calificación de 3.

La administración de usuarios se encuentra centralizada en el área de seguridad de la información en una de las empresas del mismo grupo empresarial a la cual se hará referencia como «Empresa1», esto quiere decir que «VIAJES SIS» no tiene el control sobre el AMB de usuarios. Estos datos fueron obtenidos por el reporte de solicitudes que se descarga del aplicativo BUE y el reporte de gestión que el recurso documenta diariamente.

Protección de los datos

Usa herramientas de minería de roles para detectar primero los diversos conjuntos de permisos para los usuarios de toda la empresa y después modelarlos y aplicarlos de forma centralizada.

Unificación el acceso

Los grupos pueden actualizar automáticamente su pertenencia para asegurarse de que solo tengan acceso a sus recursos los usuarios que deban tenerlo30.

Proteja sus sistemas, datos y aplicaciones ante accesos no autorizados

Los servicios de gestión de accesos e identidades de IBM cubren prácticamente todos los aspectos de su empresa, incluido el suministro de usuarios, la gestión de accesos web, el inicio de sesión único de empresa, la autenticación de multifactores y la conformidad con la actividad de usuario.

«VIAJES SIS» requiere incrementar la agilidad en los procesos de negocio y mejorar la seguridad y la disponibilidad de la infraestructura que los soporta, sin embargo hoy cuenta con una complejidad ya que coexisten diversos repositorios de identidades que operan de forma independiente y con diferentes estándares, lo que da como resultado inconsistencia en los datos, apariciones de brechas de seguridad, sobrecarga en la mesa de ayuda, incumplimiento regulatorio, no conformidades por auditoria debido a la no adecuada administración de usuarios, errores en privilegios de usuarios y complejidad en el monitoreo de los accesos de los funcionarios en los diferentes sistemas. Adicionalmente, los usuarios de los servicios ya no solamente son empleados, sino también socios de negocio, terceros y clientes. De este modo queda claro que, como tal, la gestión de identidades y control de acceso no debe entenderse como una tecnología o herramienta que se implementa en una organización de forma general y con esto se obtienen los beneficios esperados.

A continuación, se relacionan las ventajas que obtendrá la empresa «VIAJES SIS» al implementar un gestor de identidades

Reduce el tiempo necesario para el cambio de privilegios de acceso o cambio de roles. Permite la revocación instantánea y segura de sus cuentas cuando finaliza su relación con la empresa.

Universidad, así como un sencillo acceso auto-servicio de gestión de contraseña a través de un navegador web o desde el login de la red.

Soporte técnico 5x8 para la solución de Gestión de Identidad y 7x24 para la solución Access Manager .

Dos cursos virtuales certificados IBM Security Identity Governance and

Pueden mantener un control estricto sobre el acceso de los usuarios a las aplicaciones y supervisar cuidadosamente cómo los derechos se alinean con los roles y las responsabilidades del negocio.

Identity Manager basados en la tecnología IBM Data Integrator.

Informes de auditoría

Incluye Security Identity Manager para administración de contraseñas y necesidades de

aprovisionamiento complejas.

Clasificación de acceso basada en el riesgo.

TI, los auditores y los propietarios de la empresa controlar el acceso y garantizar la conformidad con la normativa

Mejor visibilidad y control del acceso de usuarios mediante la consolidación de las autorizaciones de acceso desde las aplicaciones de destino y empleando algoritmos sofisticados para la minería, el modelado y la optimización de roles.

Manager y herramientas de terceros.

Configuración de la integración con la fuente de datos .

Configuración de objetos persona

Configuración de reportes. Configuración de roles corporativos.

Levantamiento de información, diseño y documentación de las integraciones a realizar

Configuración del adaptador . Configuración de la gestión de roles para la aplicación. Configuración de las reglas de ciclo de vida de los roles. Configuración de políticas de IDs y contraseña.

Configuración de reglas de reglas de ciclo de vida de aplicación. Configuración de los reportes de la aplicación.

Servicio de Soporte

El servicio incluye la atención de incidentes/solicitudes de servicio y consultas a través de llamadas telefónicas, correo electrónico, visitas en sitio. Niveles para la atención de incidentes y solicitudes de servicio.

Severidad

Basado en esta información se establece la prioridad de resolución y el plan de escalamiento.

Para llevar a buen término la implementación de ISIGI se requiere

No se incluyen actividades de levantamiento de dicha información. Proveer información, datos, decisiones y aprobaciones requeridas para la ejecución del servicio dentro de los plazos propuestos o acordados durante la ejecución del servicio. Participar en las reuniones de estado de avance del servicio con el equipo de ETEK, cuando sea requerido.

Este contrato se utilizará por parte de ETEK en caso de ser necesario reportar problemas a los laboratorios.

Responsables

El cliente deberá asignar una persona responsable del proyecto, quien será la encargada de interactuar con el Consultor de ETEK, para la resolver todas las inquietudes durante la instalación.

El Cliente debe proporcionar la infraestructura requerida según el capítulo de arquitectura

En el caso en donde se necesite negociar otro mecanismo de integración en su mayoría webservice debido a que el cliente o el fabricante de la aplicación a integrar no concede los permisos para acceder directamente a las tablas de seguridad de la aplicación, el cliente debe proveer dicho mecanismo de la mano de su proveedor de aplicaciones. Tramitar el respectivo permiso de ingreso a las instalaciones para el personal de ETEK INTERNATIONAL en la fecha y hora acordadas para la ejecución de la actividad. Contar con la presencia y/o remota del personal de la empresa encargado de administrar la plataforma.

Los entregables en medios electrónicos a los cuales ETEK se hace responsable como parte de los servicios propuestos son

Actas de servicios . Acta e informe de cierre del proyecto.

Gestion de incidentes

Son los incidentes, los que básicamente corresponden a eventos no deseados que se detectan en la red o en los servicios y que pueden poner en riesgo uno o todos los aspectos básicos de la seguridad de la información, es decir, la disponibilidad, la confidencialidad y la integridad de la información. La gestión de incidentes permite al equipo de seguridad tener un soporte sólido para sustentar ante la alta gerencia un plan de inversión en seguridad de la información, considerando que con evidencias y los respectivos cálculos sobre impactos económicos ante la materialización de un incidente, es posible presentar de forma clara las posibles soluciones para la mitigación, ya sea correctiva o preventiva de estos eventos no deseados, logrando de esta forma que la inversión cubra las brechas de seguridad más importantes para la organización, y por consecuencia permitir una medida de la eficacia de sus controles. Promueve la aplicación del gobierno de seguridad de la información https://www.welivesecurity.com/la-es/2015/01/22/beneficios-asignacion-de-responsabilidadesseguridad-informacion/ El gobierno de seguridad está relacionado con las responsabilidades y prácticas que ejerce la alta dirección en materia de seguridad, al tiempo que se establece la participación de los distintos roles a través de la declaración de sus actividades más relevantes.

Establece el compromiso con la protección de la información

Del mismo modo, se concientiza sobre los riesgos relacionados con la información y la forma en la que pueden contribuir para su protección permite establecer el alcance y los límites de cada uno de los roles participantes, al tiempo que define a los encargados de rendir cuentas sobre las acciones que se deban ejecutar o sobre las decisiones que se hayan tomado.

Contribuye a definir las directrices de seguridad de la información

Otro beneficio está relacionado con las metas que desean alcanzarse dentro de la organización, utilizando como un habilitador a la seguridad de la información.

Https://www.cic.es/seguridad-informatica-empresa/ Tabla 17. Escala de medición Gestion de usuarios.

El robo de credenciales de acceso a sistemas es uno de los objetivos primarios o por qué puede convertirse en un riesgo inminente para la seguridad. El gobierno de Identidad le permitirá establecer la base para la estrategia de gestión de identidades a partir de la definición de roles y de accesos según el concepto de «menor privilegio». La automatización se enfoca en el aprovisionamiento y desaprovisionamiento automático de los accesos y en prestar servicios básicos como el reinicio de una contraseña o la posibilidad de solicitar un nuevo acceso de forma rápida sin ir en contravía de las políticas de seguridad de la organización y la definición de los roles. Otra recomendación es la creación de un área de seguridad de la información al interior de la compañía, que permita tener un control en línea de los usuarios y los diferentes accesos a los sistemas de la organización, como también evitar la administración compartida de los sistemas con terceros que puedan llegar a generar inconsistencia en la asignación de permisos de los funcionarios.

BIBLIOGRAFIA

Seguridad de la información. Redes, informática y sistemas de información . Implantación de un sistema de gestión de seguridad de la información ISO 27001 FC . Pdf
http://www.noticiasrcn.com/nacional-regiones-centro/millonaria-estafafalsos-planes-viaje
http://www.eltiempo.com/colombia/medellin/alerta-por-1-000-posiblesagencias-de-viajes-falsas-41700
https://www.elheraldo.co/ciencia-y-tecnologia/en-colombia-habrian-sidoafectadas-instituciones-del-gobierno-y-la-banca-en-el
https://www.oracle.com/lad/products/middleware/identitymanagement/overview/index.html
http://web.usbmed.edu.co/usbmed/fing/v3n1/v3n1a3.pdf
https://www.cic.es/seguridad-informatica-empresa
https://www.welivesecurity.com/la-es/2015/01/22/beneficios-asignacion-deresponsabilidades-seguridad-informacion/
https://www.whitebearsolutions.com/por-que-implantar-un-sistema-degestion-de-identidad-open-source-wbsvision/ 10.