Iniciar

Ciberseguridad y documentación de incidentes

Las empresas pueden verse expuestas a eventos e incidentes de seguridad que pueden poner en riesgo sus activos digitales. Una forma de minimizar esos riesgos es implementar buenas prácticas organizacionales, que lleven a crear estándares y modelos de referencia orientados a documentar procesos dentro del sistema de gestión de seguridad de la información, realizar auditorías y lograr trazabilidad informática.

Iniciar

PRIMARIO
#D3D3D3

ACENTO CONTENIDO
#FFF2BF

SECUNDARIO
#0D2380

ACENTO BOTONES
#FC502D

NEUTRAL 1
#EFEFEF

NEUTRAL 2
#F9F7EC

Introducción

Apreciado aprendiz, bienvenido a este componente formativo, donde encontrará los requerimientos asociados a la documentación de incidentes en ciberseguridad. Esta es necesaria para registrar operaciones de redes de datos; obtener la información destinada a elaborar informes y reportes relacionados con las herramientas de protección, y minimizar riesgos a los que puede verse expuesta la información.

En el siguiente video conocerá, de forma general, la temática que se estudiará a lo largo del componente formativo.

VIDEO

1 Documentación de incidentes en la Ciberseguridad

Los procesos que permiten gestionar y dar tratamiento a los incidentes de la ciberseguridad se rigen bajo la familia de las normas ISO/IEC 27000. Estas normas describen lineamientos para el seguimiento de eventos, incidentes y acciones que llevan a impactar en el desempeño de los sistemas de seguridad de la información en las empresas.

En Colombia, está contemplado dentro del marco de gobierno digital el Modelo de Seguridad y Privacidad de la Información - MSPI. Este modelo está basado en un ciclo de operación que incluye 5 fases:

- Diagnóstico
- Planificación
- Implementación
- Evaluación de desempeño
- Mejora continua

En la siguiente figura, se puede observar el ciclo de operación y las fases.

Figura 1
Ciclo de operación del modelo de seguridad y privacidad de la información

Nota. Tomada de MinTIC, 2016, p. 20.

Estas fases, logran que las entidades que implementen el MSPI gestionen de manera adecuada la seguridad y privacidad de los activos digitales, de este modo, la Estrategia de Gobierno en línea, permite centrarse en los componentes de Tecnología de la Información y Comunicaciones TIC para gestionar aquellos que incluyen la formulación, gestión e implementación de un modelo de seguridad enfocado en salvaguardar la disponibilidad, integridad, transparencia y confidencialidad de los activos y datos digitales, mediante buenas prácticas de documentación de eventos e incidentes, dando cumplimiento a los objetivos y misión de la entidad.

Los sistemas de gestión sostenibles adoptados por las entidades, generan la percepción y aceptación de un estado más transparente, abierto al público, participativo y colaborativo, garantizando que la información entregada al ciudadano cuenta con controles y criterios de seguridad, documentado cada incidente que altere o modifique algún dato dentro del universo de información almacenada.

1.1 Informes de operación de red de datos

De acuerdo con las etapas del MSPI en su fase de diagnóstico, se identifica la operatividad de la red de datos según procedimientos técnicos y marcos de referencia. Así, se describe el estado de la entidad, el nivel de madurez y el levantamiento de información, teniendo en cuenta las requerimientos, metas y resultados.

En esta etapa, al elaborar los informes de operación de la red de datos, se deben describir las metas, los resultados e instrumentos utilizados, tal como muestra en la siguiente figura y tabla.

Figura 2
Fase de diagnóstico MSPI

Nota. Tomada de MinTIC, 2016, p. 21.

Tabla 1
Fase de diagnóstico

Metas	Resultado	Instrumentos MSPI
Establecer el estado actual de la entidad en la gestión de seguridad y privacidad de la información - SPI	Herramienta diligenciada y documentada	Herramienta de diagnóstico
Identificar el nivel de madurez de SPI en la Entidad	Herramienta diligenciada y nivel de madurez identificado	Herramienta de diagnóstico
Identificar vulnerabilidades técnicas y administrativas, las cuales serán los insumos para la planificación	Informe con los hallazgos obtenidos de las pruebas de vulnerabilidad	Herramienta de diagnóstico

Nota. Tomada y adaptada de MinTIC, 2016, p. 22.

Para el desarrollo eficiente de esta fase, las entidades necesitan seguir estos pasos:

Recolectar la información a través de la herramienta de diagnóstico.

En la **fase de planificación**, se utilizan como insumos los resultados de la etapa de diagnóstico para elaborar los informes con el método de SPI, con el objetivo de determinar los procesos que se deben implementar a través del SPI, mediante la estructura de gestión del riesgo en la operación de la red de datos.

La Entidad es la encargada de limitar los procesos a ejecutar para la implementación de SPI. Estos procesos deben ser universales y abarcar todos los departamentos de la entidad. Es preciso que el alcance y limitantes respecten el cumplimiento de los objetivos, protegiendo la calidad de la información y los servicios, sobre todo la documentación de acuerdo a los informes de la operatividad en la red de datos.

A continuación, se detalla el proceso de la etapa de planificación y las partes que debe contener un informe de gestión, junto con sus metas, resultados e instrumentos para el MSPI en una entidad.

Como se puede observar, la fase de planificación contiene 4 subprocesos: Contexto, liderazgo, planeación y soporte.

Figura 3
Fase de planificación MSPI

Nota. Tomada de MinTIC.

Contexto:

Se debe conocer, investigar y hallar oportunidades de mejora dentro del MSPI, para determinar los alcances del mismo.

Liderazgo:

Planeación:

Soporte:

1.2 Documentación de implementación

En este ítem se aborda la etapa de implementación del MSPI, donde se logrará llevar acabo la implementación de lo planificado en los informes de operación de red de datos. Esta etapa contiene 3 subprocesos como son: Control y planeación operacional, plan de tratamiento de riesgos de seguridad y privacidad de la información, y la definición de indicadores de gestión.

Figura 4
Fase de implementación MSPI

Nota. Tomada de MinTic.

1 **Control y planeación operacional**

La entidad planifica, implementa y controla todos los procesos indispensables que permitan cumplir con todas las condiciones necesarias de SPI. Es indispensable, que toda esta información sea documentada para llevar un control de acciones en búsqueda de la mitigación de riesgos que puedan presentarse.

2 Plan de tratamiento de riesgos de SPI

3 Definición de indicadores de gestión:

Por otro lado, es importante definir las actividades para migrar de los protocolos IPv4 a IPv6. Cabe recordad que las ipn son las conexiones de internet. La IPv4 es más antigua y vulnerable, a partir de 2020 se migrará a IPv6. En esta fase se realizan actividades de direccionamiento, diseño, montaje, ejecución y corrección de pruebas, activación de políticas de SPI y validación de funcionalidad.

La siguiente tabla describe la meta, el resultado y el instrumento para la migración de ipv4 a ipv6.

Tabla 2
Migración ipv4-ipv6

Metas	Resultado	Instrumentos MSPI
Implementar la estrategia de migración IPv4 a IPv6.	Informe para implementar la estrategia de migración de IPv4 a IPv6	Guía Transición de IPv4 a IPv6 para Colombia

Nota. Tomada de MinTIC, 2016, p. 30.

1.3 Informes de operación de herramientas de protección

Existen herramientas de protección que permiten la operación continua de la entidad, es indispensable documentar cada etapa del proceso y generar informes, este aspecto hace parte del MSPI en las etapas de evaluación de desempeño y mejora continua.

En la etapa de evaluación de desempeño se realiza el seguimiento al MSPI, de acuerdo a los resultados obtenidos en la etapa de implementación. Este proceso permite verificar la eficiencia de todas las acciones que se implementan.

La figura 5 muestra la fase de evaluación de desempeño MSPI.

Figura 5
Fase de evaluación de desempeño MSPI

Nota. Tomada de MinTic, 2016, p. 31.

Como se puede observar, la etapa de evaluación de desempeño contiene 3 fases a su vez actividades, metas y resultados que permite la consolidación de los indicadores.

Actividades

- Revisar actividad de controles.
- Revisar evaluación por nivel de riesgo.
- Hacer seguimiento a las actividades ejecutadas.
- Hacer seguimiento a la implementación del MSPI.
- Hacer seguimiento a los registros.
- Medir indicadores de gestión.
- Hacer revisión a los planes de mejora.
- Especificar frecuencia, métodos, y responsables.
- Planificar y elaborar informes.
- Conservar información documentada en los informes.

Metas

- Informe plan de revisión y seguimiento.
- Informe de auditorías.

Resultados

- Documento con plan de seguimiento.
- Documento con el plan de auditorías.

Para finalizar con las etapas, se procede con la de mejora continua, que consolida los resultados de la fase de evaluación de desempeño, en busca del plan de mejoramiento continuo de SPI. Para ello se ejecutan acciones previas dirigidas a mitigar los efectos de los incidentes que se presentan.

Figura 6
Fase de mejoramiento continua MSPI

Nota. Tomada de MinTIC, 2016, p. 33.

Como se puede observar, la etapa de mejoramiento continuo consta de dos fases: acciones correctivas y mejora continua. Cada una contiene metas, resultados e instrumentos.

La tabla 3 describe las metas, resultados e instrumentos de la fase de mejoramiento continuo.

Tabla 3
Mejoramiento continuo

Metas	Resultado	Instrumentos MSPI
Realizar el plan de mejora Analizar los resultados del seguimiento. Analizar los resultados de las auditorías.	Informe con plan de mejora Informe con plan de divulgación	Guía de mejora continua

Nota. Tomada de MinTIC, 2016, p. 34.

2 Reportes de incidente de la ciberseguridad

Los reportes de incidentes tienen el propósito de identificar, evaluar y responder a eventos del sistema de información (SI). Con ellos es posible establecer criterios de valoración y determinar el estado de madurez de estos sistemas en las entidades. Existen seis niveles de madurez, que abarcan desde la inexistencia hasta la optimización.

Figura 7
Nivel de madurez

Nivel 0 - Inexistente
Desconoce o no tiene en cuenta el tema de seguridad de la información

Nivel 1 - Inicial
Reconoce que tiene problemas de seguridad y que estos necesitan ser resueltos

Nivel 2 - Repetible
Tiene procedimientos no formales de seguridad

Nivel 3 - Definido
En este nivel se realizan las fases de diagnóstico, planificación e implementación

Nivel 4 - Administrativo
Ha realizado las fases de evaluación de desempeño y mejora continua

Nivel 5 - Optimizado
Encuentra en la seguridad de la información, un valor agregado para la Entidad

Nota. Tomada de MinTIC, 2016, p. 35.

Inexistencia
- No se implementa control de infraestructura del SI, física, y de recursos humanos.
- No se reconoce la información como un activo digital sensible e importante.

Inicio

Repetición

Definición

Administración

Optimización

2.1 Auditorías

En muchas oportunidades no se aprecia el alto grado de exposición a vulnerabilidades en ciberseguridad que enfrentan las entidades día tras día, es por ello, que lo más idóneo es realizar una auditoría. Estas acciones que van enmarcadas a través de buenas prácticas normalizadas por ISO 27000, permite detectar, enlistar y documentar aquellas incidencias y vulnerabilidades en la infraestructura TIC de la entidad. Los objetivos de las auditorías son:

- Analizar situación actual de la entidad y rendimiento de la productividad.
- Realizar una propuesta de seguridad física perimetral.
- Analizar y planear la mejora técnica de la red interna.
- Analizar el hardware, software, y comunicaciones que ayude a generar las políticas de actualización y vulnerabilidades de la entidad.
- Enlistar las recomendaciones de mejora continua y buenas prácticas en la configuración y acceso al hardware.
- Realizar pruebas de huella externa (*Fase External Footprinting* - FEF).
- Realizar pruebas de ficheros remotos RFI.
- Probar los servidores, firewall y PC's, mediante escáner y pruebas manuales de autenticación.
- Analizar red inalámbrica (Wireless) con el fin de saber, que operación realiza una persona que acceda a esta red.
- Realizar un documento que describa las medidas a implementar y las acciones preventivas de mantenimiento en *hardware* y *software*.

El objetivo de las auditorías no es el de realizar actividades puntuales, sino acciones continuas que logran disminuir, minimizar y bloquear las amenazas latentes que están en continua transformación. De este modo, la entidad estaría preparada para actuar o prevenir consecuencias que se puedan presentar y así mejorar continuamente la seguridad y privacidad de los datos. Entre los tipos de auditorías más populares encontramos:

Hacking ético | Auditoría web | Auditoría de la red | Auditoría de código | Auditoría de código

Hacking ético
Se realiza una serie de ciberataques para detectar la vulnerabilidad de la entidad.

Todas las entidades, sin importar su tamaño, requieren de auditorías de ciberseguridad. Mantener operativa y segura la infraestructura tecnológica produce confianza en los usuarios y elevan los niveles de calidad y productividad dentro de esta. A continuación, se presentan las acciones que no pueden faltar en las auditorías de ciberseguridad.

En conclusión, una auditoría en ciberseguridad sirve para tener conocimiento e identificar algunos factores al interior de la entidad, tales como:

2.2 Marco Jurídico y Marco Legal

En la actualidad, existen diversos instrumentos Normativos de Ciberseguridad, con los cuales, el gobierno busca regular y controlar los ciberataques y los ciberdelincuentes; Entre los decretos, leyes y artículos se destacan:

CONPES 3701 de 2011 | Ley 527 de 1999 | Ley 594 de 2000 | Ley 679 de 2001

CONPES 3701 de 2011

Lineamientos de política para la ciberseguridad y ciberdefensa. Este documento establece los lineamientos para desarrollar estrategias del orden nacional con el objetivo de contrarrestar las amenazas informáticas.

Para ampliar la información y a manera de ejemplo, se puede referir a los anexos:

Anexo 1
MARCO JURÍDICO CIBERSEGURIDAD PONAL
Descargar

Anexo 2
Comercio sobre la Ciberdelincuencia - LEY 1928 DE JULIO 24 DE 2018
Descargar

2.3. Herramientas de gestión y manual de funcionamiento

Para que los sistemas no sufran consecuencias tras los ataques de ciberseguridad, es importante contar con herramientas de protección y, además, que los encargados de estas cuenten con las habilidades y conocimientos para su óptimo funcionamiento.

Software antivirus | *Firewall* | *Proxy* | *PKI - Public Key Infrastructure* | *MDR – Managed Detection and Response* | *Pentesting*

Software antivirus
Estos programas permiten contar con medidas de protección efectivas cuando el equipo se encuentre expuestos a software malicioso o cualquier otro tipo de malware; Estos programas ofrecen la oportunidad de eliminarlo por completo o poner en estado de cuarentena.

Software antivirus. Para conocer la herramienta y su manual de funcionamiento, se puede remitir a este enlace.

Documentación de los procesos

Para conocer las características de la documentación que deben soportar los procesos, ver el video a continuación.

VIDEO

Recuerde explorar los demás recursos que se encuentran disponibles en este componente formativo; para ello, diríjase al menú principal, donde encontrará la síntesis, una actividad didáctica para reforzar los conceptos estudiados, material complementario, entre otros.

Control de la seguridad digital

Síntesis: Ciberseguridad y documentación de incidentes

El siguiente mapa integra los criterios y especificidades de los conocimientos expuestos en el presente componente formativo.

Actividad didáctica

Ciberseguridad y documentación de incidentes

Esta actividad le permitirá determinar el grado de apropiación de los contenidos del componente formativo.

De acuerdo con la definición planteada en la columna izquierda, arrastre cada término al lugar que considere correcto de la columna derecha.

Arrastrar y soltar

Realizar

Inicio

- Se hace una aproximación a las debilidades y fallencias del SI.
- Las incidencias son tratadas de manera reactiva.
- Se detecta la necesidad de implementar el MSPI.

Repetición

- Se identifica y clasifica de manera general los activos de información.
- Se crea la cultura de consciencia del SI entre los funcionarios.
- Todo lo relacionado con DPI es tratado en cuestión de gestión.
- La actividad ingresa de lo ad-hoc y cuenta con una planeación.

Definición

- Diagnóstico del estado del SI.
- Determinación de objetivos, acciones y alcances del SI.
- Establecimiento de políticas, procedimientos, roles y responsabilidades del SI y divulgación de toda la entidad.
- Inventario de activos de información.
- Implementación de un plan de tratamiento de riesgo.
- Alineación de la# 4 y 6 y documentación del plan de transición.

Administración

- Revisión y monitoreo periódico de activos de información.
- Uso de indicadores KPI para complimiento de políticas de SPI.
- Evaluación de la efectividad de las acciones orientadas a disminuir incidentes, errores y/o posibles fraudes.
- Pruebas constante del del del SPI.

Optimización

- La seguridad como valor agregado para el cumplimiento de metas en la entidad.
- La información como un valor único e inalienable.
- La información con criterios de transparencia, claridad, oportunidad, integridad y disponibilidad.
- Uso de indicadores para mejorar comportamos innovantes.
- Tallers, tips.

Hacking ético | Auditoría web | Auditoría de la red | Auditoría de código | Auditoría de código

Auditoría web

Es alguien que detectar la seguridad del servidor y la página web de la entidad.

Hacking ético | Auditoría web | Auditoría de la red | Auditoría de código | Auditoría de código

Auditoría de la red

Calcular el firmware de los sistemas operativos y dispositivos. Revisar procesos de control e internet y mapa de conexiones de la entidad.

Hacking ético | Auditoría web | Auditoría de la red | Auditoría de código | Auditoría de código

Auditoría de código

Revisar pruebas de código a las App que se usan en la entidad.

Hacking ético | Auditoría web | Auditoría de la red | Auditoría de código | Auditoría de código II

Auditoría de código II

Hacer pruebas de conexión y vulnerabilidad de los dispositivos conectados a la red corporativa.

CONPES 3701 de 2011 | Ley 527 de 1999 | Ley 594 de 2000 | Ley 679 de 2001

Ley 527 de 1999

Validez jurídica y probatoria de la información electrónica. Leyes donde se reglamenta el acceso y uso a los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.

CONPES 3701 de 2011 | Ley 527 de 1999 | Ley 594 de 2000 | Ley 679 de 2001

Ley 594 de 2000

Ley General de Archivos. Establece las reglas y principios generales que regulan la función archivística del Estado.

CONPES 3701 de 2011 | Ley 527 de 1999 | Ley 594 de 2000 | Ley 679 de 2001

Ley 679 de 2001

El objetivo de esta ley es prevenir y contrarrestar la explotación, la pornografía, el turismo sexual y demás formas de abuso sexual con menores de edad, mediante normas de carácter preventivo y sancionatorio.

Ley 527 de 1999 | Ley 594 de 2000 | Ley 679 de 2001 | Ley 962 de 2005

Ley 962 de 2005

Simplificación y racionalización de trámites y procedimientos administrativos para facilitar las relaciones de los particulares con la Administración pública.

Ley 594 de 2000 | Ley 679 de 2001 | Ley 962 de 2005 | Ley 1150 de 2007

Ley 1150 de 2007

Seguridad de la información en contratación pública. Modifica la Ley de 80 1993 y dicta otras disposiciones generales aplicables a toda contratación con recursos públicos.

Ley 679 de 2001 | Ley 962 de 2005 | Ley 1150 de 2007 | Ley 1266 de 2008

Ley 1266 de 2008

Habeas data. Desarrollo el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos.

Ley 962 de 2005 | Ley 1150 de 2007 | Ley 1266 de 2008 | Ley 1273 de 2009

Ley 1273 de 2009

Protección de información de los datos. Crea el marco contra los atentados a la confidencialidad, integridad y disponibilidad de los datos.

Ley 1150 de 2007 | Ley 1266 de 2008 | Ley 1273 de 2009 | Ley 1341 de 2009

Ley 1341 de 2009

Principios y conceptos sobre la sociedad de la información y la organización de las TIC. Determina el marco general para la formulación de las políticas públicas que regirán el sector de las TIC y su ordenamiento general.

Ley 1266 de 2008 | Ley 1273 de 2009 | Ley 1341 de 2009 | Ley 1437 de 2011

Ley 1437 de 2011

Procedimientos Administrativos y de lo Contencioso Administrativo. Protege y garantiza los derechos y libertades de las personas ante las actuaciones de las autoridades y de la Administración en ejercicio de sus actividades y la Constitucion y demás principios del ordenamiento jurídico.

Ley 1273 de 2009 | Ley 1341 de 2009 | Ley 1437 de 2011 | Ley 1480 de 2011

Ley 1480 de 2011

Estatuto del Consumidor. Protege al consumidor de medios o mercado electrónico.

Ley 1341 de 2009 | Ley 1437 de 2011 | Ley 1480 de 2011 | Decreto Ley 019 de 2012

Decreto Ley 019 de 2012

Racionalizar trámites a través de medios electrónicos. Suprime o reforma regulaciones, procedimientos y trámites innecesarios existentes en la Administración pública.

Ley 1437 de 2011 | Ley 1480 de 2011 | Decreto Ley 019 de 2012 | Ley 1581 de 2012

Ley 1581 de 2012

Protección de datos personales. Desarrollo el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos o archivos.

Ley 1480 de 2011 | Decreto Ley 019 de 2012 | Ley 1581 de 2012 | Ley 1712 de 2014

Ley 1712 de 2014

Transparencia y derecho al acceso a la información pública nacional. Regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.

Decreto Ley 019 de 2012 | Ley 1581 de 2012 | Ley 1712 de 2014 | Decreto 2364 de 2012

Decreto 2364 de 2012

Firma electrónica. Reglamenta el medio de identificación electrónica flexible y tecnologicamente neutro que se adecúa a los necesidades de la sociedad.

Ley 1581 de 2012 | Ley 1712 de 2014 | Decreto 2364 de 2012 | Decreto 2609 de 2012

Decreto 2609 de 2012

Expediente electrónico. Fortalece los archivos públicos del país, para garantizar la eficacia de la gestión del Estado y la conservación del patrimonio documental.

Ley 1712 de 2014 | Decreto 2364 de 2012 | Decreto 2609 de 2012 | Decreto 2693 de 2012

Decreto 2693 de 2012

Sistema de Líneas Conceptuales, planeo y términos para garantizar el máximo aprovechamiento de los recursos de información, el intercambio de información y de la sinergia en la coordinación en el Estado más eficiente, más transparente y participativo.

Decreto 2364 de 2012 | Decreto 2609 de 2012 | Decreto 2693 de 2012 | Decreto 1377 de 2013

Decreto 1377 de 2013

Protección de datos. Reglamenta parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.

Decreto 2609 de 2012 | Decreto 2693 de 2012 | Decreto 1377 de 2013 | Decreto 1510 de 2013

Decreto 1510 de 2013

Sistema de compras y contratación pública. Las entidades estatales deben procurar el logro de los objetivos del sistema de compras y contratación pública definidos por Colombia Compra Eficiente.

Decreto 2693 de 2012 | Decreto 1377 de 2013 | Decreto 1510 de 2013 | Decreto 333 de 2014

Decreto 333 de 2014

Entidades de certificación. Define el régimen de acreditación de las entidades de certificación

Software antivirus | *Firewall* | Proxy | PKI - Public Key Infrastructure | MDR - Managed Detection and Response | Pentesting

Firewall

Cuarto paso prevenir y contrarrestar la red privada de ataques de otras redes. Es funcionamiento en varios niveles incluyendo los siguientes de red, permitidos/rechazo y filtrado/bloqueo según las reglas definidas por un administrador.

Firewall: Para conocer la herramienta y su manual de funcionamiento, ya puede verlo a este enlace.

Software antivirus | *Firewall* | *Proxy* | PKI - Public Key Infrastructure | MDR - Managed Detection and Response | Pentesting

Proxy

Programa o dispositivo Firewall que actúa de intermediario entre conexiones del Ciudadano e Internet. Filtrando todos los paquetes entre ambos.

Proxy: Para conocer la herramienta y su manual de funcionamiento, ya puede verlo a este enlace.

Software antivirus | *Firewall* | Proxy | ***PKI - Public Key Infrastructure*** | MDR - Managed Detection and Response | Pentesting

PKI - Public Key Infrastructure

Herramienta para el intercambio de datos de forma segura a través de Internet. Es un sistema criptográfico de una pareja.

PKI - Public Key Infrastructure: Para conocer la herramienta y su manual de funcionamiento, ya puede verlo a este enlace.

Software antivirus | *Firewall* | Proxy | PKI - Public Key Infrastructure | ***MDR - Managed Detection and Response*** | Pentesting

MDR - Managed Detection and Response

Servicio de seguridad gestionado, que proporciona la búsqueda y monitoreo constante de amenazas.

MDR - Managed Detection and Response: Para conocer la herramienta y su manual de funcionamiento, ya puede verlo a este enlace.

Software antivirus | *Firewall* | Proxy | PKI - Public Key Infrastructure | MDR - Managed Detection and Response | ***Pentesting***

Pentesting

Pruebas hechas por expertos mantiene técnicas avanzadas para detectar vulnerabilidades en los sistemas con permiso dañino que las amenazas informáticas pueden aprovechar.

Pentesting: Para conocer la herramienta y su manual de funcionamiento, ya puede verlo a este enlace.

Portada actividad

800 x 800

Portada actividad

800 x 800

Imagen acompañamiento Actividad

600 x 600

Imagen Resultado

900 x 600

Implementar las pruebas de efectividad.

Documentar el resultado del diagnóstico.

Determinar el nivel de madurez.

Éstos resultados necesitan ser revisados y divulgados por todas las personas que intervienen en el proceso para iniciar con la siguiente fase.

En el marco de apropiación del MSPI, los líderes y directores de las entidades deben propender porque todos los funcionarios acaten y sientan el compromiso de dar fiel cumplimiento a la normatividad, asignando roles y responsabilidades en cada uno de los aspectos a tratar.

Planeación:

Plantear acciones y objetivos, de tal manera que se cree la hoja de ruta para abordaje de eventos e incidentes.

Soporte:

Documentar la entrega de recursos y competencias a cada área de manera oficial, mediante sensibilizaciones y comunicaciones.

Plan de tratamiento de riesgos de SPI

Es indispensable la implementación del plan de tratamiento de riesgos, en donde se debe identificar los controles aplicar para que éstos lleguen a un nivel aceptable.

Definición de indicadores de gestión

Los indicadores sirven para medir la eficiencia y efectividad en las acciones implementadas en SPI y lograr una mejora continua.