1. OBJETIVO:

Desarrollar un plan de gestión de riesgos tecnológicos que administra y brinda los servicios tecnológicos e informáticos, dentro del sistema SGI de la Escuela Superior Tecnológica de Artes Débora Arango.

2. ALCANCE

Lograr el compromiso de la **ESCUELA SUPERIOR TECNOLOGICA DE ARTES DEBORA ARANGO**, para emprender la implementación del plan de gestión del riesgo en la seguridad de la información. Designar funciones de liderazgo para apoyar y asesorar el proceso de diseño e implementación del plan de gestión. Capacitar al personal de la entidad en el proceso de plan de gestión del riesgo de la seguridad de la información**.**

3. RESPONSABLE

Jefe de Recursos Tecnológicos y de Apoyo Académico

4. DEFINICIONES

Gestión de riesgos: El proceso de ponderación de las distintas opciones normativas a la luz de los resultados de la evaluación de riesgos y, si fuera necesario, de la selección y aplicación de las posibles medidas de control apropiadas, incluidas las medidas reglamentarias.

Esta definición de la gestión de riesgos, que se ha propuesto incluir en el Manual de procedimiento del Codex Alimentarius (4), toma en cuenta todos los elementos (enumerados más abajo) que pueden constituir el proceso de gestión de riesgos (evaluación de riesgos, evaluación de las opciones para la gestión de riesgos, aplicación de la decisión sobre gestión, y seguimiento y examen de la misma). Sin embargo, en la práctica no siempre será necesario incluir todos estos elementos. Por ejemplo, es probable que la adopción de las decisiones nacionales sobre gestión de riesgos comprenda todos los aspectos mencionados en la definición, mientras que generalmente las actividades del Codex en materia de gestión de riesgos no comprenden los aspectos de aplicación, seguimiento y examen.
Política de evaluación de riesgos: Directrices para los juicios de valor y elecciones normativas que pueden necesitarse en determinadas fases decisorias del proceso de evaluación de riesgos.

El establecimiento de la política de evaluación de riesgos constituye una tarea de gestión de riesgos, que debe desempeñarse en estrecha colaboración con los asesores de riesgos y sirve para proteger la integridad científica de la evaluación de riesgos. Se debe documentar que las directrices adoptadas garantizan la coherencia y la transparencia. Algunos ejemplos de establecimiento de políticas de evaluación de riesgos son la identificación de la(s) población(es) expuesta(s) al riesgo, la determinación de criterios de clasificación de los peligros, y las directrices para la aplicación de factores de seguridad.
Perfil del riesgo: Descripción del problema de inocuidad alimentaria y de su contexto.

El trazado de perfiles de los riesgos es el proceso mediante el cual se describe un problema de inocuidad de un alimento, así como su contexto, a fin de identificar los elementos del peligro o el riesgo que revisten interés para las distintas decisiones de gestión de riesgos. El perfil del riesgo incluirá la identificación de aquellos aspectos de los peligros que resultan pertinentes a efectos de la asignación de prioridades y del establecimiento de la política de evaluación de riesgos, así como los aspectos del riesgo que revisten importancia para la elección de las normas de inocuidad y opciones en materia de gestión.

Un perfil de riesgo típico podría incluir los siguientes elementos: breve descripción de la situación y del producto o producto básico en cuestión; valores que se considera que estarán expuestos a riesgo (por ej., salud humana, aspectos económicos); posibles consecuencias; percepción de los riesgos por parte del consumidor; y distribución de los riesgos y beneficios

5. CONTENIDO

PLAN DE GESTION DEL RIESGO EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Recursos Tecnológicos y de Apoyo Académico

Ciudad: Envigado-Antioquia - Colombia

Elaboró:

Marcos Alejandro Niño Reyes

Débora Arango
Escuela Superior Tecnológica de Artes

Considerando la situación actual de los recursos tecnológicos, los principales servicios y actividades que se realizan a diario con la finalidad de mitigar las fallas y amenazas que atentan contra la seguridad de los equipos y de la información, ya que aún no se han definido una política de seguridad ni procesos que aseguren la continuidad de los servicios.
Para la consecución del objetivo principal se han definido los siguientes objetivos específicos:
Determinar el alcance del plan de riesgos propuesto, ya que no se cuenta con toda la documentación necesaria como pueden ser datos estadísticos de incidentes, entrevistas al personal, entre otros que permitan conocer más de cerca la situación de riesgo; el trabajo propuesto considerará los principales aspectos que puedan afectar a la pérdida o deterioro de la información.
Definir los principales activos que forman parte del modelo de negocio de la institución, como son los equipos, lugares y aplicaciones de software que en conjunto permiten una buena administración de la institución para fines administrativos, académicos y financieros.
Identificar las principales amenazas que afectan a los activos anteriormente considerados, pudiendo afectar la integridad, disponibilidad y confiabilidad de la información que estos almacenan o transfieren.
Proponer salvaguardas para minimizar los riesgos que pudiesen materializarse tras las amenazas definidas anteriormente.
Desarrollar un plan de gestión de seguridad y privacidad que permita minimizar los riesgos de pérdida de activos de la información en la ESCUELA SUPERIOR TECNOLOGICA DE ARTES DEBORA ARANGO.

LIMITACIONES:

Crear el rubro del presupuesto necesario para apoyar la implementación del plan de gestión del riesgo de la seguridad de la información en la ESCUELA SUPERIOR TECNOLOGICA DE ARTES DEBORA ARANGO.

IMPORTANCIA DE LA GESTIÓN DE RIESGOS

En el ámbito empresarial se está dando mayor prioridad a salvar, proteger y custodiar el activo de la información, debido a que los sistemas de información y los avances tecnológicos están siendo implementados en todas las empresas.
En la ESCUELA SUPERIOR TECNOLOGICA DE ARTES DEBORA ARANGO, sigue los lineamientos trazados por el Gobierno Nacional en cumplimiento de la Ley de Transparencia 1712 de 2014 y Gobierno en Línea que viene impulsando actividades dentro de las entidades públicas para que se ajusten a modelos y estándares que permitan brindar seguridad a la información dando cumplimiento al Decreto 1078 de 2015.
Los riesgos por desastres naturales, riesgos inherentes relacionados con procesos no adecuados en el tratamiento de la misma información, desconocimiento de normas y políticas de seguridad y el no cumplimiento de estas, suelen ser los temas más frecuentes y de mayor impacto presentes en las entidades. Una entidad sin un plan de gestión de riesgos está expuesta a perder su información.
Todas las organizaciones deberían implementar planes para gestionar los riesgos que afectan a los sistemas de información, tecnologías de información y activos informáticos, considerando que en la actualidad los riesgos más comunes son generados por ataques dirigidos al software empresarial, afectando la disponibilidad e integridad de la información almacenada o transportada a través de los equipos de comunicación.
Por esta razón hay que estar preparados para prevenir todo tipo de ataques o desastres, ya que cuando el costo de recuperación supera al costo de prevención es preferible tener implementados planes de gestión de riesgos que permitan la continuidad del negocio tras sufrir alguna pérdida o daño en la información de la entidad.
Considerando la situación actual de LA ESCUELA SUPERIOR TECNOLOGICA DE ARTES DEBORA ARANGO, para reducir los niveles de riesgo, es indispensable diseñar un plan para iniciar las prácticas de las normas y políticas de seguridad e implementar procesos que aseguren la continuidad de los servicios.

DEFINICION GESTIÓN DEL RIESGO

La definición estandarizada de riesgo proviene de la Organización Internacional de Normalización (ISO), definiéndolo como “la posibilidad de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y por lo tanto causa daño a la organización”.

VISION GENERAL PARA LA ADMINISTRACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

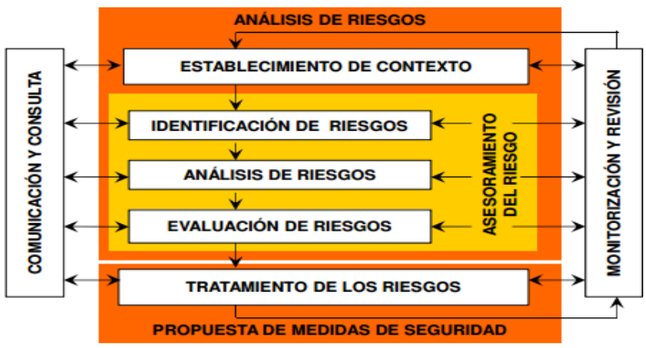


Figura 1 Proceso para la administración del riesgo.

IDENTIFICACIÓN DEL RIESGO

1. Riesgo Estratégico: Se asocia con la forma en que se administra la entidad. El manejo del riesgo estratégico se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.
2. Riesgos de Imagen: Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.
3. Riesgos Operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad y de la articulación entre dependencias.
4. Riesgos Financieros: Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.
5. Riesgos de Cumplimiento: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad, de acuerdo con su misión.
6. Riesgos de Tecnología: Están relacionados con la capacidad tecnológica de la entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.

SITUACION NO DESEADA

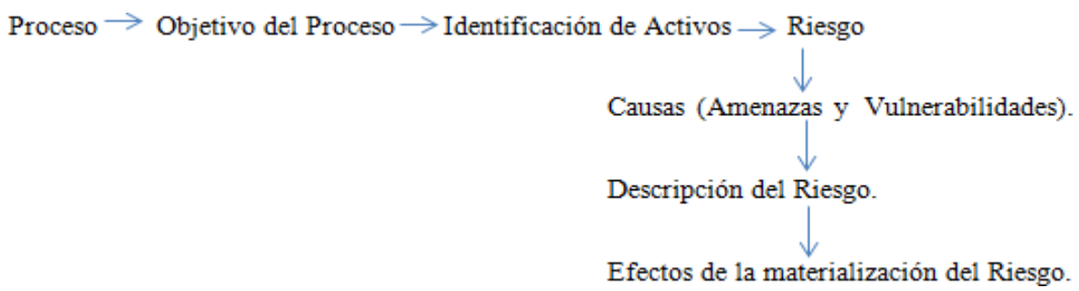
- Hurto de información o de equipos informáticos.
- Hurto de información durante el cumplimiento de las funciones laborales, por intromisión Incendio en las instalaciones de la empresa por desastre natural o de manera intencional.
- Alteración de claves y de información.
- Pérdida de información.
- Baja Cobertura de Internet.
- Daño de equipos y de Información.
- Atrasos en la entrega de información, atrasos en asistencia técnica
- Fuga de información
- Manipulación indebida de información

ORIGEN DEL PLAN DE GESTION

Es necesario crear un plan de gestión de riesgos de seguridad de la información que permita proteger el activo más valioso para la entidad; la información.
La situación actual del sistema de seguridad de la información en la entidad se encuentra planteado en el diagnóstico de seguridad y privacidad de la Información.
El gobierno nacional y el ministerio de las TIC han abanderado los proyectos de Gobierno en Línea que permite conocer el funcionamiento de las alcaldías y entidades públicas en el país. Es por ello necesario que LA ESCUELA SUPERIOR TECNOLOGICA DE ARTES DEBORA ARANGO, cumpla con los requisitos necesarios para entregar la información de manera oportuna y eficiente a estas entidades, a la población y comunidad en general.

PROPÓSITO DEL PLAN DE GESTION DE RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN.

Dar soporte al modelo de seguridad de la información al interior de la entidad. Conformidad legal y evidencias de la debida diligencia.
Preparación de un plan de respuesta a incidentes.
Descripción de los requisitos de seguridad de la información para un producto un servicio o un mecanismo.
Alcances, límites y organización del proceso de gestión de riesgos en la seguridad de la información.



ANALISIS DE VULNERABILIDADES/DESCRIPCIÓN DE VULNERABILIDADES

- La red de internet implementada por conexión WiFi cubre un 96 %, y en unas áreas la señal es débil ya que debe atravesar paredes y los espacios son grandes y contamos con aulas insonorizadas, que es difícil el acceso de la señal.
- Los puntos de red ubicados en cada oficina no son suficientes y se han dispuesto nuevos según se va presentando la necesidad.
- Algunos cables de energía están sueltos, no están cerca a los escritorios o no son suficientes para la cantidad de equipos que tiene cada oficina, existe riesgo de pérdida de información en el caso que sean desconectados por accidente y la información procesada por el funcionario no alcanza a ser guardada.
- Bebidas y alimentos (se debe generar campañas de sensibilización) que cerca de los equipos de cómputo, cualquier derrame de líquidos afectan los equipos informáticos y su información.
- La información es llevada en memorias o discos duros portátiles personales, por ende, la información sale de la entidad.
- No hay control para el uso de memorias portátiles en los equipos de la institución, exponiendo a perder la información por virus no detectados o daños irreparables del hardware.
- Existe una cantidad de documentos físicos que se manejan en la entidad y no se han digitalizado, los custodia el área de Gestión documental, en archivadores especializados.

- No existe un plan de continuidad de negocio que permita reanudar las operaciones normales durante o después de interrupciones significativas a las operaciones de la institución (en caso de incendio o desastre natural existen altas probabilidades de perder la información de los servidores)
- La institución cuenta con 3 UPS de energía que soportan las caídas luz, pero se requiere adquirir más equipos con mayor autonomía.

MATRIZ DE VULNERABILIDADES Y MITIGACION DEL RIESGO

					ANALISIS		**VALORACION**	**VIGENCIA DE CUMPLIMIENTO**
VULNERABILIDAD	DESCRIPCIÓN	CAUSA	EFECTO	CLASIFICACION	CALIFICACION	EVALUACION	MITIGACION DEL RIESGO	
*Fallas eléctricas	Las conexiones no son suficientes, no cumplen con las exigencias el tamaño de la red de equipos de cómputo (cables sueltos, inadecuada estructura y adecuación)	Inadecuada conexión de cableado eléctrico	Posible pérdida de información	*Riesgo tecnológico *Riesgo físico *Riesgo humano	40	Riesgo moderado	Debido al cambio de sede un nuevo diseño de la red eléctrica	Vigencia 2018
*Afectación de activos de información y activos informáticos.	Desconocimiento de las políticas y normas de seguridad de la información.	No socialización No capacitación de las políticas y normas de seguridad.	Acciones no adecuadas en el tratamiento de los activos de información e informáticos	* Riesgo Tecnológico * Riesgo en Servicio * Riesgo de la Información * Riesgo en personal	60	Riesgo Alto	Diseñar, socializar e implementar un Manual de políticas y normas de seguridad de la información en la alcaldía municipal.	Vigencia 2018
*Pérdida de información *Pérdida de tiempo productivo en funciones laborales.	La red implementada no es la más adecuada para la estructura física de la alcaldía y la cantidad de equipos informáticos. Las fallas en la señal de internet son constantes.	Señal inalámbrica	Señal débil en las oficinas. Retraso en Tiempos de producción para los funcionarios.	*Riesgo Tecnológico *Riesgo en servicio *Riesgo de información.	40	Riesgo Importante	Implantar un modelo de red basado en cableado estructurado.	Vigencia 2018

					ANALISIS		**VALORACION**	**VIGENCIA DE CUMPLIMIENTO**
VULNERABILIDAD	DESCRIPCION	CAUSA	EFECTO	CLASIFICACION	CALIFICACION	EVALUACION	MITIGACION DEL RIESGO	
Incumplimiento de las actividades de seguridad de la información.	El personal encargado de los sistemas no es suficiente. No se están siguiendo protocolos y normas para garantizar la seguridad de la información en la entidad.	No existe personal encargado del proceso de aseguramiento de la información	Ausencia de transferencia de conocimiento y falta d e capacitación	*Riesgo de información. *Riesgo de servicio. *Riesgo tecnológico	60	Riesgo Alto	Encargar a personal capacitado para el aseguramiento de la información. Capacitar al personal de la alcaldía municipal para el cumplimiento de procesos y actividades de seguridad de la información	Vigencia 2018
Confidencialidad e Integridad de la información	En la entidad se trabaja en la campaña cero papel, sin embargo se han encontrado dentro del papel reutilizable información personal de algunos pobladores del municipio beneficiarios de Programas sociales.	Exposición de datos personales en papel Reutilizable.	incumplimiento de confidencialidad e integridad de la información	*riesgo de Información	60	Riesgo Alto	Socializar con los funcionarios de la entidad acerca de las políticas de seguridad y confidencialidad de la información.	Vigencia 2018
Perdida total de Información	No se cuentan con los tipos de extintores adecuados Para cada necesidad.	No se cuentan con los tipos de extintores adecuados para cada Necesidad.	*No hay extintores *La planta de energía no funciona	*Riesgo de Información. *Riesgo de Servicio. *Riesgo tecnológico	60	Riesgo Alto	Adquirir los extintores necesarios. Revisar el funcionamiento y puesta en marcha de la planta de energía	Vigencia 2018

Tabla 1. MATRIZ DE VULNERABILIDADES Y MITIGACION DE RIESGOS

VULNERABILIDAD	**DESCRIPCION**	**CAUSA**	**EFECTO**	**CLASIFICACION**	**ANALISIS**		**VALORACION**	**VIGENCIA DE CUMPLIMIENTO**
					CALIFICACION	EVALUACION	MITIGACION DEL RIESGO	
*Pérdida de Información	Los funcionarios no realizan copias de seguridad a la información producto de sus funciones.	No hacen copias de seguridad	Posible pérdida de información	*Riesgo de Información * Riesgo en Servicio	4 0	Riesgo Importante	*Crear un instructivo de copias de seguridad *Capacitar al personal de la alcaldía municipal para el dominio de este tema. *Adquirir un servidor para almacenar las copias de seguridad. *Adquisición de una nube para almacenamiento de información. *Crear cuentas de usuario con claves.	Vigencia 2018
	Equipos compartidos en algunas secretarías	No existen cuentas de usuario.						Vigencia 2018
*Pérdida de Información	Uso de memorias extraíbles y unidades extraíbles	No hay control de uso	Infección por Virus	*Riesgo Tecnológico				Vigencia 2018
*Perdida de información	El Datacenter no cuenta con todas las especificación exigidas para el correcto funcionamiento y adecuación de un área de tal importancia.	Incendios, ingreso de personal no autorizado, posible robo de servidores,	Perdida d e información por catástrofe o riesgo en manos	*Riesgo en Servicio *Riesgo en información	4 0	Riesgo Moderado	Adecuación del Datacenter de la alcaldía Municipal, cumpliendo con las características exigidas por normas y estándares en Colombia. (Piso falso, cámara de seguridad, extintores adecuados, entre otros)	Vigencia 2018
*Pérdida de información y/o deterioro físico	La documentación e información en papel o	No se ha iniciado la ejecución de	Daño de documentos y	*Riesgo de Información	40	Riesgo Importante	Iniciar la ejecución de la digitalización y	Vigencia 2018

	física está siendo archivada en sitios no adecuados para Ello.	Digitalización de información.	Deterioro del papel.				almacenamiento de la información contenida en papel.	
No hay respaldo de información en sistemas de información	No existe un proceso establecido de copias de seguridad dentro y fuera de la entidad para la información generada en los sistemas de información. No Existe un sistema de información para la documentación sensible, Como contratos y acuerdos.	No hay procesos de copias de seguridad establecidos	Perdida de información	*Riesgo Tecnológico *Riesgo de información	60	Riesgo Importante	*Crear procesos de copias de seguridad. *Invertir en un software o sistema de información para el almacenamiento y consulta de la documentación física existente en la alcaldía.	Vigencia 2018
Transición IPv4 a IPv6	No existen transición de protocolo de IP	No existen transición de protocolo de IP	No existen transición de protocolo de IP	*Riesgo tecnológico	20	Riesgo Bajo	*establecer normas para la transición de IPv4 a IPv6 debido a que todos los equipos informáticos de la entidad soportan la nueva versión de IP	Vigencia 2018

PROPUESTA DE SEGURIDAD

- Se debe fortalecer la red inalámbrica actual, para minimizar el problema de internet lento y caídas de señal.
- Revisar, organizar y ubicar las conexiones de electricidad según las necesidades propias de las oficinas, ya que tenemos evidencias de saturación de conexiones eléctricas, en la sede No. 01
- Replantear las políticas de seguridad y privacidad de la información como también las políticas de seguridad informática.
- Revisar las políticas existentes para identificar debilidades y fortalezas, si es necesario se hacen ajustes, teniendo en cuenta que seguridad informática no es igual a seguridad de la información.
- Socializar las políticas de seguridad y privacidad de la información con el personal de la Institución.
- La creación de un comité de informática que dirija la creación y el control de un sistema de seguridad y privacidad de la información en la institución junto con otras actividades propias del área de TIC.
- Crear los procesos de la oficina de las TIC para la entidad.

- Implementar el sistema de documentación digital en la institución para reducir riesgos de pérdida de información física por ser documentación de años o de vigencias muy viejas.
- La institución comprometida con la campaña cero papel, en las compras de tecnología de las vigencias 2018 y 2019 adquirirá nuevos escáner de alta velocidad, con el fin de digitalizar los documentos y que sea más información digital que impresa.

PLAN FORTALECER LAS COPIAS DE SEGURIDAD DE LA INSITIUCIÓN

- Obtener una nube dedicada para la información de la institución con el fin de tener un respaldo en caso de accidentes en los servidores de La institución.
- Contar con un plan alternativo que asegure la continuidad de la actividad del negocio en caso que ocurran incidentes graves, como incendios o calamidades por desastres de tipo natural.
- Nunca se debe olvidar que la realidad es que la entidad puede sufrir un incidente que afecte su continuidad y, dependiendo de la forma en que se gestionen dichos incidentes, las consecuencias pueden ser más o menos graves. Siempre teniendo en cuenta que la información requiere ser protegida y se debe trabajar sobre los tres pilares fundamentales: confidencialidad, integridad y disponibilidad. Una de las principales características que debe poseer la entidad es buscar cómo establecer un sistema de seguridad enfocado por procesos, resaltando la importancia que tienen las actividades de monitoreo y la correcta configuración para disminuir los riesgos y realizar tratamiento de las diferentes y constantes vulnerabilidades, para lo cual se deberán tener en cuenta los hallazgos y recomendaciones identificadas, cuyo propósito se encamine a mitigar los riesgos encontrados.

PLAN DE CONTINUIDAD DEL NEGOCIO

- Diseñar un formato de chequeo de acuerdo a las necesidades de la organización que permita realizar las auditorías periódicas con la finalidad de verificar que los objetivos de control, procesos y procedimientos se cumplan.

- Socializar con los directivos, y las distintas áreas de la institución, la importancia del Plan de Continuidad de Negocio, para hacer frente a incidentes graves de seguridad en

la entidad, resumiendo de forma clara y sencilla cada una de las actividades a desarrollar dentro del plan.

- Diseñar estrategias para el proceso de recuperación teniendo en cuenta los tiempos de reacción e implementación de contingencias ante la realización de los eventos identificados.
- Adoptar una de las tres posiciones, que permita minimizar la ocurrencia o los efectos colaterales sobre la red, esto de acuerdo con los siguientes enfoques:

1) Detectar el riesgo

2) Plantear controles y efectuar las implementaciones respectivas.

3) Mitigar el riesgo

- Diseñar un plan de contingencia teniendo en cuenta que la continuidad en el negocio dependerá de los riesgos y amenazas potenciales que serán tratados de acuerdo a lo siguiente:

1) Política de copia de seguridad de datos

2) Procedimientos de almacenamiento fuera de la institución

3) Procedimientos de gestión de emergencias, por desastre natural, por incendio o por inundaciones.

IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD PARA LA INFORMACIÓN

El análisis permitió identificar que se desconocen y poco se cumplen las políticas de seguridad; por lo cual debe quedar integrado con el documento actual. Se recomienda entre otros tener en cuenta:

- Socialización y capacitación de temas de seguridad.
- Ambiente con la seguridad física adecuada.
- Sistemas de respaldo para mantener soporte de la información en caso de eventualidades catastróficas.

PLAN DE CAPACITACIÓN

Contar con un plan de capacitación para el personal encargado de la seguridad de la información, aspectos a fortalecer como:

1) Detectar los requerimientos tecnológicos

2) Determinar objetivos de capacitación para personal

3) Evaluar los resultados monitoreados del sistema de seguridad.

4) Elaborar un programa de capacitación en temas de ciberseguridad y políticas de seguridad de la información para todos los funcionarios de la entidad.
5) Evaluar los resultados de cada actividad.

10. PLAN DE TRANSICIÓN DE IPV4 A IPV6

Se debe establecer un plan para hacer la transición de las direcciones IPv4 existente actualmente por la IPv6, se requieren tener en cuenta para seguir el proceso de transición de IPv4 a IPv6, en
Las distintas organizaciones del estado, teniendo en cuenta su aplicación para todo el ciclo de desarrollo por fases que requiere el nuevo protocolo, en un ambiente controlado y seguro que permita consolidar una adopción del protocolo IPv6 con éxito en el país.
Para abordar esta temática se empezará por comentar que desde hace más de tres décadas, las redes de telecomunicaciones han venido creciendo exponencialmente generando una mayor demanda de servicios y oportunidades en la red mundial de internet; con el aumento de las tecnologías computacionales y de comunicaciones, ha aumentado el proceso de innovación tecnológica en los diversos dispositivos
Tanto alámbricos como inalámbricos, como por ejemplo, celulares, puntos de acceso, tabletas, servidores, equipos de almacenamiento entre otros, que
comenzaron a incrementar la conectividad en muchas redes en el mundo y para ello han tenido que hacerlo con direcciones de internet que permiten establecer conexiones para cada elemento conectado a la red, estas direcciones se conocen como direcciones IP (Internet Protocol Versión 4), que en estos momentos entraron a una fase de agotamiento final, así mismo en el año 1992 la Internet Engineering Tas Force IETF1 a partir de diversos grupos de trabajo definió el RFC 2460
(Especificaciones del Protocolo Internet Versión 6 (IPv6) que dio origen al nuevo Protocolo de conectividad denominado IPv6 o Ipng (Next Generation Internet Protocol).
En ese orden de ideas el protocolo IPv6, hace posible que todos los dispositivos tecnológicos usados para la conexión a internet, tengan una dirección en IPv6, la cual facilitará la conectividad en banda ancha, ofreciendo mejores servicios poniéndolos al alcance de toda la población a fin de estimular y ofrecer mejores oportunidades para el desarrollo mundial.

CONCLUSIONES

El seguimiento constante a los procesos y la implementación del plan de mitigación de riesgo de seguridad de la información deben ser ejecutados, monitoreados y actualizados frecuentemente.

Es indispensable implementar el plan de gestión de riesgo que permitirá prevenir las posibles amenazas encontradas en la infraestructura tecnológica de la entidad.

Las políticas de seguridad de la información de LA ESCUELA SUPERIOR TECNOLOGICA DE ARTES DEBORA ARANGO, deben ser revisadas y actualizadas conforme al crecimiento, cambios de la estructura organizacional, exigencias del gobierno y los mismos procesos dentro de la entidad.

6. REGISTRO DE MODIFICACIONES

VERSIÓN	FECHA	ITEM MODIFICADO	DESCRIPCIÓN