PLAN DE CAPACITACIÓN Y DIVULGACIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

MARÍA FERNANDA AYALA ZAPATA
Contralor

EQUIPO OFICINA DE INFORMATICA

CONTRALORIA GENERAL DE SANTIAGO DE CALI
SANTIAGO DE CALI
2020

Contenido

Índice de Ilustraciones 3
1 GLOSARIO. 4
2 INTRODUCCIÓN. 7
3 ALCANCE. 7
4 OBJETIVOS. 7
4.1 Objetivo General: 7
4.2 Objetivos específicos. 7
5 MARCO DE REFERENCIA 8
5.1 Marco Conceptual. 8
5.1.1 Información. 8
5.1.2 Seguridad de la información. 8
5.1.3 El Factor Humano en la seguridad de la Información. 9
5.2 Técnicas para la Comunicación de la Información. 10
5.2.1 Técnicas para la Comunicación del Material de Entrenamiento. 10
5.2.2 Entrenamiento Web. 10
5.2.3 Entrenamiento en Sitio Presencial. 11
5.2.4 Entrenamiento Basado en Computador. (CBT) 11
5.2.5 Entrenamiento por Medio de Video Interactivo. 11
6 DESCRIPCIÓN GENERAL DEL PLAN DE CAPACITACIÓN Y DIVULGACIÓN. 11
7 DISEÑO ..... **¡Error! Marcador no definido.**
7.1 Modelo ..... **¡Error! Marcador no definido.**
7.2 Definición de Roles, Temáticas y Priorización. ..... **¡Error! Marcador no definido.**
7.2.1 Roles involucrados y Responsabilidades. ..... **¡Error! Marcador no definido.**
- Comité Directivo: ..... **¡Error! Marcador no definido.**
- Proceso informático: ..... **¡Error! Marcador no definido.**
- Funcionarios de La Contraloría General Santiago de Cali: ..... **¡Error! Marcador no definido.**

7.2.2 Priorización.....**¡Error! Marcador no definido.**

7.2.3 Temáticas del Plan de Capacitación de Seguridad y privacidad de la Información Vigencia 2020-2021. .....**¡Error! Marcador no definido.**

Generalidades sobre la información: .....**¡Error! Marcador no definido.**

Conocimiento de las políticas de seguridad de la información: ..... **¡Error! Marcador no definido.**

Amenazas informáticas: .....**¡Error! Marcador no definido.**

7.3 Objetivos del Plan de Capacitación y Divulgación de la Seguridad y privacidad de la Información. .....**¡Error! Marcador no definido.**

7.4 Diseño del Plan de Capacitación y Divulgación..... **¡Error! Marcador no definido.**

7.5 Cronograma de Actividades. .....**¡Error! Marcador no definido.**

8 DESARROLLO. .....**¡Error! Marcador no definido.**

8.1 Desarrollo del Material para la Capacitación. ..... **¡Error! Marcador no definido.**

8.2 Desarrollo del Material para la Divulgación. **¡Error! Marcador no definido.**

9 IMPLEMENTACIÓN .....**¡Error! Marcador no definido.**

9.1 Socialización con la Alta Dirección. 12

9.2 Implementación de las Divulgaciones. 13

9.3 Implementación de las Capacitaciones. 13

9.4 Evidencias de las Capacitaciones. 13

9.5 Definición de Métricas. 13

10 MEJORAMIENTO DEL PLAN DE CAPACITACIONES. 14

10.1 Monitoreo de la Realización de las Divulgaciones 14

10.2 Monitoreo de la Realización de las Capacitaciones 14

10.3 Evaluación de las Actividades de Capacitación. 14

10.4 Aplicación de los Resultados de la Encuesta. 15

11 INDICADORES. 15

12 BIBLIOGRAFÍA. 17

Índice de Tablas.

Tabla 1 cronograma .....**¡Error! Marcador no definido.**
Tabla 2 indicadores..... 16
Tabla 3 Firmas Revisores. 17

Índice de Ilustraciones

Ilustración 1 Fases del Plan de Capacitación. 12

1. GLOSARIO.

Backup: es un respaldo que se tiene implementado para información o software de manera que se pueda retomar su uso normal generando la menor latencia posible.
Contingencia: Suceso que puede suceder o no, especialmente un problema que se plantea de forma imprevista.

Dominio de Servicios Tecnológicos: Define estándares y lineamientos para la gestión de la infraestructura tecnológica que soporta los sistemas y los servicios de información, así como los servicios requeridos para su operación. Comprende la definición de la infraestructura tecnológica, la gestión de la capacidad de los servicios de TI, la gestión de la operación y la gestión de los servicios de soporte.

Estándares: Especificaciones técnicas que tienen una función instrumental y que responden a como se implementa un lineamiento o elemento.

Gobierno Digital: Se refiere al uso creativo de las tecnologías de información para transformar la manera como interactúa el Gobierno con las empresas y los ciudadanos.

Sensibilización: es un proceso mediante el cual se muestra el valor que tiene para determinado proceso u organización el impacto de algún otro evento.

Hardware: Denominada como “parte dura del computador”, es el conjunto de elementos físicos tanto internos como externos de un computador, como un ejemplo de elementos externos están: teclado, pantalla, mouse, impresora, etc. Como un ejemplo de partes internas están: memoria RAM, discos duros internos, memoria cache, etc.

Lineamientos: Son una orientación de carácter general, corresponden a una disposición o directriz que deben ser implementadas en las entidades correspondientes.

Máquina virtual: Es un software que simula una computadora de manera que permite ejecutar diferentes sistemas operativos montados unos encima de otros pero conservando el nivel de independencia deseado entre ellos. Una característica esencial de las máquinas virtuales es que los procesos que ejecutan están limitados

por los recursos y abstracciones proporcionados por ellas. Estos procesos no pueden escaparse de esta "computadora virtual".

Obsolescencia: La obsolescencia tecnológica hace referencia a la necesidad de recambio de un aparato tecnológico, el producto ha llegado al final de su vida útil esto aplica tanto para el hardware como para el software.
Software Multiplataforma: se conoce como software multiplataforma aquel que no depende del sistema operativo para su funcionamiento de manera que la misma unidad aplicativa puede ejecutarse sobre cualquier sistema operativo. La mayoría de software multiplataforma depende de máquinas virtuales como por ejemplo la JVM o máquina virtual de java.

Software: Denominada como “parte blanda del computador”, son los diferentes programas que se ejecutan sobre el hardware de la computadora, hacen parte del hardware tanto los diferentes sistemas operativos como los programas de aplicaciones que se ejecutan sobre ellos.

Vulnerabilidad: La palabra vulnerabilidad hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos.

Política: Declaraciones de alto nivel en los que se expresan los deber ser de la entidad sobre un tema en particular.

Información: es el nombre por el que se conoce un conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Virus Informático: Un virus informático es un programa o fragmento de código diseñado para provocar daños en un equipo corrompiendo archivos del sistema, despilfarrando recursos, destruyendo datos o alterando el funcionamiento normal de otra forma.

Malware: El malware o software malicioso es un tipo de software que tiene como objetivo infiltrarse o dañar un sistema de información sin el consentimiento de su propietario.

El término se utiliza para hablar de todo tipo de amenazas informáticas o software hostil, y existen distintos tipos de malware en función de su origen y consecuencias. Entre ellos nos encontramos con los virus, gusanos, troyanos, keyloggers, botnets, spyware, adware, ransomware y sacareware.

Antivirus: Originalmente, un programa antivirus era un software que detectaba y en ocasiones eliminaba virus informáticos de los dispositivos infectados, y por lo tanto también contribuía a detener la propagación del contenido malicioso. Eso era

sobre todo en los 1990s y a principios de los 2000. Sin embargo, debido al enorme crecimiento del número de malware en otras categorías, los programas antivirus han evolucionado hacia soluciones de seguridad compleja.

Ciberseguridad: Es la práctica de defender las computadoras y los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos.

2. INTRODUCCIÓN.

Las organizaciones, tanto públicas como privadas, están dando especial trato al recurso tecnológico, esto a razón de que este componente ha tomado gran importancia dado que la tecnología de información es una herramienta que brinda mayor competitividad y genera valor a todas sus partes interesadas.

El problema que se origina en este punto, es que con todo el valor que genera a todo nivel, vienen inmersos una gran cantidad de riesgos que de no ser atendidos de manera oportuna por personal de todo nivel en la Contraloría General de Santiago de Cali, la institución se podría ver inmersa en diferentes situaciones como: suplantaciones de identidad, infecciones masivas de virus, salida de circulación de la página web, etc.

Muchas veces, las empresas cometen errores por los que se deben pagar altos precios y podrían ser fácilmente evitables desarrollando políticas bien orientadas y capacitando a todo su personal en ellas, esto hace necesario sensibilizar y capacitar sobre la importancia de la preservación de la disponibilidad, integridad y confidencialidad de la información.

3. ALCANCE.

El plan de seguridad de la información aplica para la capacitación y divulgación de la seguridad y privacidad de la información a todos los funcionarios de La Contraloría General de Santiago de Cali para el periodo comprendido entre enero 2020 hasta diciembre del año 2021.

4. OBJETIVOS.

4.1 Objetivo General:

Este documento tiene como objetivo presentar el plan de capacitación y divulgación de seguridad y privacidad de la información para la Contraloría General de Santiago de Cali tomando como fecha inicial el año 2020 y tomando como objetivo el final del periodo de la actual administración (2020-2021).

4.2 Objetivos específicos.

- Definir los temas necesarios para la capacitación de los diferentes públicos objetivo.

- Establecer la metodología con la que se implementaran las diferentes los diferentes eventos.
- Definir los materiales que serán usados para las capacitaciones.
- Realizar la adecuada divulgación de los temas concernientes a las capacitaciones.

5. MARCO DE REFERENCIA

El marco de referencia para elaborar este documento se basa en la norma internacional ISO 27001, que da los lineamientos en cuanto al aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.
Dentro de la norma se destaca que todos los planes y medidas que se tomen para proteger y asegurar la información, se deben complementar con las buenas prácticas de seguridad de la información por parte de las personas que hagan uso de los sistemas y los datos, para que así los controles o medidas a tomar sean realmente efectivas.

5.1 Marco Conceptual.

5.1.1 .Información.

La información es la base de la sociedad moderna como la conocemos, con en esta podemos solucionar problemas, tomar decisiones, o debatir los existentes, y determinar cuál alternativa de un conjunto de ellas es la que mejor se adapta a nuestras necesidades.
La información es el escalón medio de la escalera del conocimiento, está conformada por un conjunto de datos con significado que están supervisados y ordenados, que con un debido filtrado, gestión y actualización, convierten la información en conocimiento.

5.1.2 Seguridad de la información.

La seguridad de la información es el grupo de acciones que realizan las organizaciones buscando el resguardo y la adecuada protección de la información, pretendiendo mantener sus características para que esta sea confiable, las acciones para proteger la integridad de la información suelen ser de dos tipos: preventivos y reactivos.
Una buena Gestión de la Seguridad de la Información busca conservar a nivel general las características principales de la información que son: seguridad, confidencialidad, integridad y disponibilidad.

Para una correcta gestión, se debe tener en cuenta que la seguridad de la información no se da como algo puntual ni un hecho de facto, debe ser visto como un proceso continuo que hay que gestionar conociendo siempre las vulnerabilidades y las amenazas a las que está expuesta la información.

5.1.3 El Factor Humano en la seguridad de la Información.

Para entender el papel que juega el factor humano en la seguridad de la información hay que ver la entidad como una maquinaria, que está conformada por áreas o dependencias y cada una de estas cumple una función o proceso, y a su vez se interrelacionan entre sí para hacer que la Contraloría General de Santiago de Cali Funcione.

En cada parte del engranaje que hace que la entidad opere, hay personas realizando labores de diferentes maneras, en el caso de la Contraloría General de Santiago de Cali más del 99% de sus actividades se realizan a través de medios tecnológicos como los computadores.

Si hacemos la analogía de ver a los funcionarios como piñones que forman parte de un engranaje, haría falta hacerles mantenimiento para que el engranaje funcione correctamente, en el caso de las personas no se les puede lubricar o ajustar con llaves, pero lo que haría las veces de mantenimiento es la capacitación de ese personal para que adquiera nuevas habilidades y afiancen las ya adquiridas, por tal motivo es fundamental la formación continua de las persona para que aumenten sus competencias, y directamente aumente la competitividad y eficiencia de la entidad. Teniendo en cuenta que la información es un activo que requiere gestión, es necesario tener funcionarios capacitados en buenas prácticas de seguridad de la información para evitar pérdidas o corrupción de la misma en el futuro.

Observemos las ventajas que se obtienen al tener un personal capacitado:

- Aprovechamiento de las herramientas y controles de seguridad.
- Confianza en los datos que son el insumo de la labor.
- Integración de todos con el tema.
- Aseguramiento en todos los niveles de la información.
- Reduce pérdidas potenciales de información.
- Permite la mejora continua del SGSI.
- Facilita la gestión de los profesionales en informática.
- Garantiza calidad y transparencia en los procesos.

Po último se debe resaltar que si se invierten millones en software especializado, seguridad y profesionales capacitados, no habrán resultados positivos si las personas que utilizan los sistemas no hacen el primer filtro de seguridad,

protegiendo contraseñas, evitando los spyware, teniendo protocolos de navegación y de descarga de archivos entre otros, porque para que haya corrupción en un sistema de información debe abrirse una puerta, y esa puerta es casi siempre abierta por las personas que los utilizan de manera inconsciente, por eso se debe tener funcionarios capacitados y conscientes.

5.2 Técnicas para la Comunicación de la Información.

Actualmente se cuentan con muchas técnicas y medios para hacer llegar un mensaje de sensibilización de manera efectiva, pero se debe tener en cuenta que la manera más adecuada depende de las necesidades de cada entidad, del tema a tratar, y de los recursos disponibles tanto de personal como de infraestructura, a continuación se brinda unas recomendaciones que servirán de base para comunicar las capacitaciones de sensibilización:

- Posters con mensajes o checklist sobre que debe y que no debe hacerse.
- Videos institucionales a través de videowalls o pantallas.
- Screensavers con mensajes de sensibilización.
- Cuadernos, relojes o elementos de oficina con mensajes alusivos.
- Boletines vía email.
- Eventos relacionados con seguridad, concursos etc.
- Sesiones con instructores (si se planean charlas que contengan varios temas de sensibilización a la vez).
- Mediante aplicativos de uso institucional.(Docunet)
- A través de la Intranet. (Mecicalidad).

5.2.1 Técnicas para la Comunicación del Material de Entrenamiento.

Las técnicas para la comunicación del material deben aprovechar la tecnología existente para facilitar la divulgación y acceso a la misma, hay ciertas técnicas que han tenido gran acogida por su fácil implementación, las cuales son:

5.2.2 Entrenamiento Web.

Es una de las técnicas más utilizadas, ya que permite a su vez de disponer el material necesario, realizar pruebas y mediciones si se diseña el sistema apropiadamente, otra de sus ventajas es que puede realizarse también a distancia.

5.2.3 Entrenamiento en Sitio Presencial.

La ventaja más evidente es el grado de interacción que provee con el instructor y el grupo. Su mayor desventaja está en el tamaño del grupo o la cantidad de grupos a capacitar. Esto puede incurrir en la necesidad de más instructores y otros gastos adicionales.

5.2.4 Entrenamiento Basado en Computador. (CBT).

Entrenamiento asistido por computador, es un entrenamiento que dependiendo de su despliegue puede requerir o no conexión a internet. Incentiva el autoestudio y brinda disponibilidad casi que permanente y desde cualquier lugar.

5.2.5 Entrenamiento por Medio de Video Interactivo.

Su ventaja principal es que permite el entrenamiento a distancia y al mismo tiempo permite la interacción con el instructor. Puede ser un método costoso.

6. DESCRIPCIÓN GENERAL DEL PLAN DE CAPACITACIÓN Y DIVULGACIÓN.

El desarrollo de este plan, se hará buscando las mejores herramientas y metodologías que puedan colaborar con la apropiación del conocimiento de seguridad y privacidad de la información de todo el personal de la institución, buscando que los funcionarios conozcan de la importancia que tiene cada uno en salvaguardar los activos de la información de la entidad, que son hoy en día el activo más importante de las empresas (tanto públicas como privadas) a nivel mundial.
Este plan, debe llevarse a cabo en 4 fases que consisten en:

- Fase de diseño.
- Fase de desarrollo.
- Fase de implementación.
- Fase de mejoramiento.

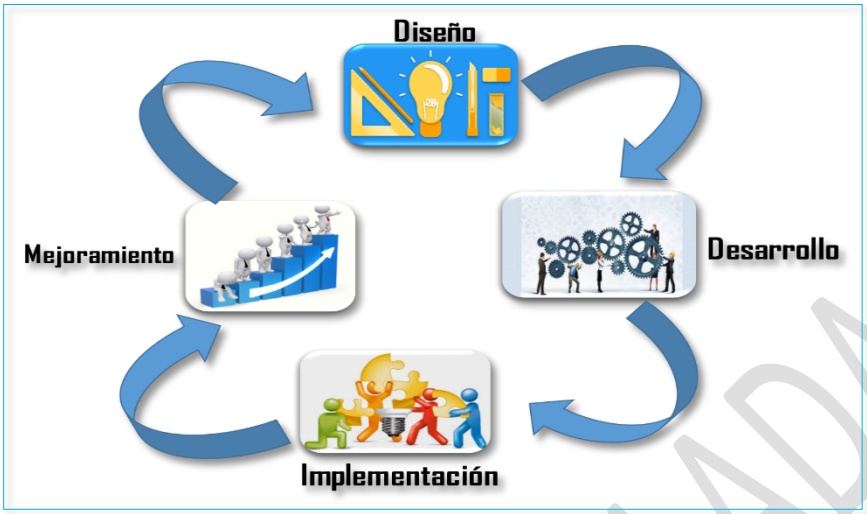

Ilustración 1 Fases del Plan de Capacitación.

A continuación, se describen cada una de las fases:

Diseño: Aquí se identifican los diferentes modelos de capacitación a aplicar, las necesidades de la entidad y las fuentes de información disponible, se dará forma a la programación que llevará a cabo el plan.

Desarrollo: Aquí se ajustarán los materiales para que sean los adecuados a la capacitación para cada nivel, buscando los logros analizados en el diseño.

Implementación: Aquí se desarrolla la metodología con la cual se le llevará el material desarrollado al público objetivo.

Mejoramiento: como todo proceso continuo, debe tener una fase de retroalimentación con el fin de que el plan no se haga obsoleto con el tiempo.

6.1 Socialización con la Alta Dirección.

Para comunicar el plan a la alta dirección se deben cumplir los siguientes requisitos:

- Tener el diseño de las capacitaciones.
- Definición de los recursos necesarios el tratamiento de los temas y el material para el desarrollo de los mismos.
- La programación con fechas y horarios.
- La cantidad de personas a capacitar.
- El medio por el cual se realizarán las exposiciones.
- Los formatos de control con los parámetros de medición.

Una vez la alta dirección de la aprobación, la capacitación puede dar inicio con los recursos que hayan sido aprobados.

6.2 Implementación de las Divulgaciones.

Las divulgaciones, se podrán llevar a cabo vía:

- correos electrónicos.
- Docunets.
- Whatsapp.
- Protectores de pantalla.
- Página web.

Estas divulgaciones realizaran según la necesidad percibida por el equipo de informática o por solicitud directa del contralor de turno, previa validación del tema a divulgar.

6.3 Implementación de las Capacitaciones.

En cuanto a las capacitaciones, estas se llevaran a cabo de manera virtual o presencial según la situación actual de la entidad, se prepararán con:

- diapositivas u otro tipo de presentaciones.
- Videos explicativos.
- Medios de comunicación impresos.
- Video conferencias.

6.4 Evidencias de las Capacitaciones.

Para dejar constancia de las asistencias a las capacitaciones, se dispondrá de un formato de asistencia y actividades, el formato se hará firmar al inicio y fin de la capacitación.
Adicionalmente, si ve la necesidad se podrá dejar un registro fotográfico o audiovisual del grupo en general que tome la capacitación.
Al firmar la planilla de asistencia, el funcionario está aceptando la cláusula que indica que han recibido la capacitación en los temas determinados sobre seguridad y privacidad de la información, y asume su responsabilidad en la preservación de la seguridad de la información.

6.5 Definición de Métricas.

Con el fin de medir la efectividad del plan de capacitaciones es necesario definir métricas que permitan evaluar la efectividad de la capacitación y divulgación, indicando aspectos cuantitativos y cualitativos como:

- Apropiación de la información.
- Claridad de la información.
- Tiempo de la capacitación.

- Dominio del tema por parte del expositor.
- Grado de satisfacción sobre el medio utilizado para la sensibilización.

La forma de recolectar la información para llevar a cabo la evaluación del plan de capacitación y divulgación se podrá realizar a través de:

- Evaluaciones o cuestionarios.
- Foros Abiertos con usuarios que recibieron la capacitación.
- Entrevistas selectivas o entrevistas grupales.
- Uso de observadores independientes o auditores, que evalúen la efectividad del programa.
- Verificación de la cantidad de incidentes abiertos y su causa
- Ataques de ingeniería social, posteriores a las capacitaciones.
- Percepciones por parte de los expositores.

7. MEJORAMIENTO DEL PLAN DE CAPACITACIONES.

Para lograr la mejora del plan de capacitaciones es necesario analizar los datos cuantitativos y cualitativos obtenidos de las métricas, para evidenciar las fortalezas del plan y las oportunidades de mejora del mismo.
Un mejoramiento exitoso no solo depende de analizar datos, también se deben tener en cuenta los avances tecnológicos, las amenazas nuevas que traen consigo y la disponibilidad de recursos para ejecutar las mejoras.

7.1 Monitoreo de la Realización de las Divulgaciones

Con el fin de llevar un adecuado control sobre las divulgaciones realizadas, por cada una de estas se diligenciará un formato de atención a usuarios que debe incluir: a quienes fue dirigido, la fecha en que se ejecutó, una breve descripción del contenido, y toda otra medida que sea necesaria para soportar la evidencia.

7.2 Monitoreo de la Realización de las Capacitaciones

Con el fin de llevar un adecuado control sobre las capacitaciones realizadas, por cada una de estas se diligenciará un formato de asistencia y actividades que debe incluir como mínimo: a quienes fue dirigido, la fecha en que se ejecutó, una breve descripción del contenido, y todo otra medida que sea necesaria para soportar la evidencia.

7.3 Evaluación de las Actividades de Capacitación.

Para la evaluación de las actividades, se realizará una prueba de conocimientos en el intermedio o al final de la capacitación (a discreción del capacitador), para evaluar la apropiación del conocimiento se podrán utilizar:

- Talleres de respuesta extensa.
- Ejercicios de selección múltiple con única respuesta.
- Ejercicios de selección múltiple con múltiple respuesta.
- Foros abiertos.

Dichas evaluaciones pueden ser realizadas también ya sea de la manera tradicional incluyendo lápiz y papel o de manera virtual.
Los asistentes también podrán evaluar la capacitación con respecto a las características de la exposición y la claridad del expositor.

7.4 Aplicación de los Resultados de la Encuesta.

Los resultados de los exámenes y encuestas se tabularán y analizaran, lo que permitirá ver la efectividad del plan, resaltando las fortalezas y debilidades del mismo.
Las oportunidades de mejora evidenciadas deben ser analizadas y clasificadas bajo el criterio de cuales tienen mayor impacto sobre el plan, y cuales tienen un menor impacto, una vez identificadas las de mayor impacto se debe presentar una propuesta de mejora donde se detalle:

- Porqué es susceptible de mejora.
- Acciones y/o medidas a aplicar.
- Recursos necesarios.
- Presupuesto requerido.

Una vez aplicada la acción de mejora se debe evaluar la efectividad de esta para determinar si es exitosa, en caso negativo se deben tomar las acciones requeridas siguiendo los parámetros ya mencionados, si el resultado es positivo se deberá continuar con la oportunidad de mejora que siga en la lista.
Este tipo de análisis se debe hacer en cada ciclo de capacitaciones y divulgaciones, para así garantizar una mayor calidad en el ciclo siguiente.

8. INDICADORES.

Con el fin de medir que tan efectivo es el plan de capacitaciones en general, se tendrán en cuenta dos indicadores que van ligados a los temas tratados, a los cuales se les hará seguimiento en los comités de coordinación y seguimiento cada trimestre.

Tabla 1 indicadores

Nombre del Indicador	Objetivo	Meta	Fórmula
Indicador de Cobertura	Medir el alcance del Plan de Capacitación y Divulgación de la Seguridad de la Información	70%	**C= (NPC/TPE)*100** **C:** Cobertura **NPC**: Número de personas capacitadas **TPE:** Total de personas objetivo
Cumplimiento	Cumplimiento de las actividades de capacitación y divulgación programada	90%	**C=(CR/CP)*100** **AS:** Cumplimiento. **CR: Capacitaciones Realizadas** **CP: Capacitaciones Programadas**

9. BIBLIOGRAFÍA.

1) Buenas prácticas en seguridad de la información. https://www.pmg-ssi.com/2017/10/iso-27001-buenas-practicas-seguridad-informacion/
2) Las amenazas informáticas más comunes. https://www.oceano-it.es/news-individual/369/amenazas-informaticas-mas-comunes-en-la-actualidad
3) Definición de información: https://es.wikipedia.org/wiki/Informaci%C3%B3n
4) Definición de virus informático: https://www.avg.com/es/signal/what-is-a-computer-virus
5) Definición de malware: https://computerhoy.com/video/que-es-malware-29917
6) Definición de antivirus: https://www.eset.com/es/caracteristicas/antivirus-software-que-es/#
7) Definición de Ciberseguridad: https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security
8) Capacitación sobre seguridad de la información: https://www.escuelaeuropeaexcelencia.com/2019/04/beneficios-de-la-capacitacion-sobre-seguridad-de-la-informacion-para-las-organizaciones/
9) Norma iso 27001: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/
10) Imagen d diseño: https://images.app.goo.gl/5Wb7AuSAWvqmkZ1LA
11) Imagen desarrollo: https://images.app.goo.gl/9ZMxjLR8C3uCym688
12) Imagen implementación: https://images.app.goo.gl/12Y5EWXWHGaYuYZn9
13) Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información MINTIC.

Tabla 2 Firmas Revisores.

	Nombre	Cargo	Firma
Proyectó	Cristian Carabali	Contratista- Técnico Operativo	
Revisó	Carlos Alfonso Lozano Caicedo	Jefe Oficina de Informática	
Aprobó	Carlos Alfonso Lozano Caicedo	Jefe Oficina de Informática	
Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad lo presentamos para firma.			