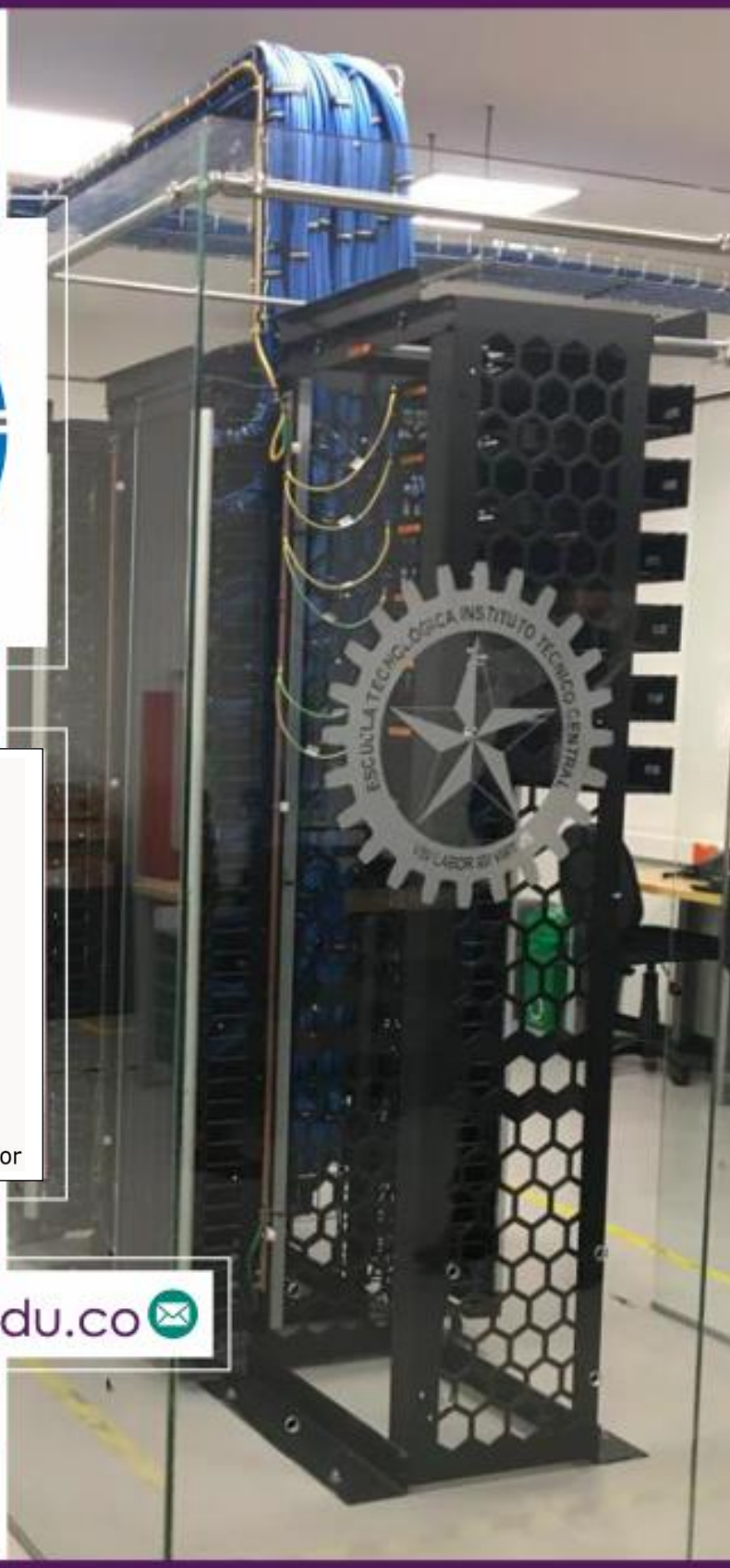
Informe de Gestión 2021
Gestión de Seguridad de la Información



Escuela Tecnológica
Instituto Técnico Central
Establecimiento Público de Educación Superior

seguridaddigital@itc.edu.co

Seguridaddigital

Lema: 2021

"Ciberseguridad, creando un mundo digital confiable"

Propósito Principal de SGSI

Desarrollar actividades relacionadas con la implementación y sostenibilidad del Sistema de Seguridad de la Información en la entidad, de conformidad con las Políticas y Lineamientos vigentes.

Para el periodo 2021 – 2024, el Plan Institucional de Desarrollo se denominó "Un nuevo acuerdo institucional, social y ambiental para la consolidación de la escuela 2021- 2024 ". La ETITC busca cumplir sus expectativas, a través de tres estrategias, 11 objetivos, 27 proyectos y 70 metas. Lo anterior permitirá que la Escuela siga formando a la niñez y a la juventud en habilidades técnicas básicas y en tecnologías disruptivas, para la transformación del país, esto tomado de las palabras de nuestro Hno. Ariosto Ardila.

Planificar: Aquí se definen las políticas de seguridad, los procesos y procedimientos para la administración del riesgo y mejoras el SGSI y que cumpla con objetivos de la ETITC.

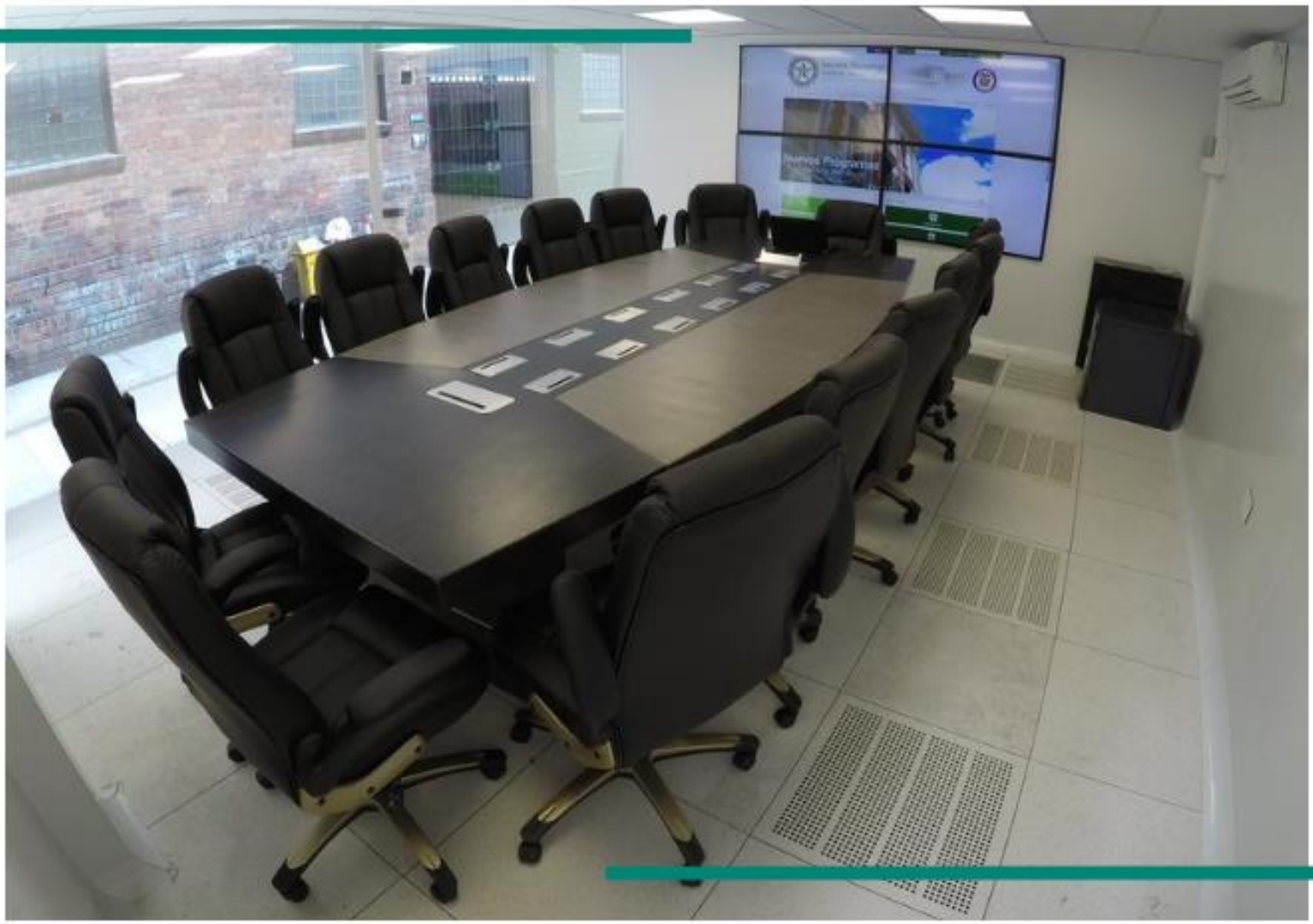
Hacer: Aquí se pone en marcha el Sistema de Gestión, implantando tecnologías, controles de seguridad, como el de actualizar procesos y procedimientos, etc.

Verificar: En esta etapa se realizan las mediciones y análisis de la efectividad de los controles de seguridad de acuerdo a revisiones de alta gerencia, de control interno, así como de auditorías ejecutados con el fin de evaluar los objetivos, experiencias e informando los resultados para su respectiva revisión.

Actuar: En esta etapa se realizan acciones correctivas y preventivas basadas en las auditorías internas y revisiones del SGSI y/o cualquier otra información relevante que nos permita realizar mejoras continuas al Sistema de Gestión de Seguridad de la Información.

Alcance de SGSI

El Sistema de Gestión de Seguridad de la Información y el Modelo de Seguridad y Privacidad de la Información, de Gobierno en Línea, se encuentran basados, en el marco de lo establecido, en la norma internacional NTC-ISO-IEC 27001:2013 y las buenas prácticas contenidas en el componente Seguridad y Privacidad de la Información, de la estrategia GEL, este último desarrollado por el Ministerio de Tecnologías de la Información y las Comunicaciones en Colombia.



Más información visitar:

https://www.etitc.edu.co/es/page/nosotros&seguridad-informacion

ACTIVIDADES EJECUTADAS

2021

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

#1 Establecer requerimientos mínimos de seguridad que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir para la entidad, de conformidad con la normatividad vigente.

Divulgación del Manual de Políticas de Seguridad y Privacidad de la Información

20. POLÍTICAS DE ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO

- 20.3- Política de Uso de Herramientas Institucionales en Teletrabajo

Actualizar el Manual de Políticas de Seguridad y Privacidad de la Información

20. POLÍTICAS DE ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO

- Complementar el item 21.2 en cuanto a las responsabilidades de los Servidores públicos, Estudiantes, Proveedores y Partes Interesadas en la Política de Privacidad y Protección de Datos Personales"

Actualización de Procedimiento GSI-PC-04
Procedimiento de Intercambio de Información Física

FECHA	VERSION	CAMBIOS
03/09/2017	1	Adopción del procedimiento
26/04/2018	2	Modificación del objetivo y alcance del procedimiento. Modificación del código
29/10/2021	3	Actualización de software de redacción de correspondencia y del nombre del procedimiento GDO-PC-01 Comunicaciones Oficiales y/o PQRSD, eliminación de paso entre 4 y 5 (ya que es un único paso)

ELABORÓ	REVISÓ	APROBÓ
SANDRA JOHANA GUERRERO GÓMEZ Líder de Gestión de la Seguridad de la Información	YANETH JIMENA PINZÓN CORTÉS Administrador de la Documentación	DORA AMANDA MESA CAMACHO Representante de la Dirección

CLASIF. DE CONFIDENCIALIDAD	IPG	CLASIF. DE INTEGRIDAD	A	CLASIF. DE DISPONIBILIDAD	1

Actualización de Normagrama a la vigencia 2021

Actualización de Mapa y Plan de Tratamiento de Riesgos

Actualización del Formato GSI-FO-01 Compromiso de Confidencialidad de la Información en cuanto al uso y Divulgación de la Información de la ETITC.

#2

Desarrollar pruebas periódicas de vulnerabilidades sobre los diferentes sistemas de información para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad, de acuerdo con las metodologías establecidas.

El 27 de Octubre de 2021, se realizó pruebas de vulnerabilidades al Sistema Académico Academusoft; donde se analizó el certificado SSL/TLS y se evidencia que este portal no proporciona la confidencialidad, integridad y autenticidad de los datos.

Se indaga a nuestro Web Master Cristian Chaparro y está es su respuesta:

Solicitud de certificado en URL

Emisora EMITC
Mié 27/10/2021 17:28
Para: Seguridad Digital ETITC

Hola;
En este caso toca consultarle a Nitza o a Omar.

Cristian David Chaparro Parra
Profesional Medios Digitales

Se remite pregunta al Profesional de Registro y Control:

Acerca del Certificado SSL Academusoft

Seguridad Digital ETITC
Mié 27/10/2021 17:34
Para: Registro ETITC

Inge Omar como estás,

En conversación con el Ingeniero Cristian, me indica que tú eres la persona que me puede apoyar en la **revisión del certificado** del Sistema de Información Académico Academusoft;

http://186.30.166.147/itec/hermesoft/portalIG/home_1/publicacion/publicado/index.htm

El Profesional de Registro y Control responde lo siguiente:

Acerca del Certificado SSL Academusoft

Registro ETITC
Jue 28/10/2021 9:41

Para: Seguridad Digital ETITC

Atento saludo Ingeniera, desde mi salida del área de sistemas me restringieron toda actividad relacionada con el área, por lo que considero que no le puedo aportar nada y menos en temas de seguridad, si a bien lo tiene y puntualmente quiere hacer me una pregunta con gusto le atiendo y si en mi ignorancia la puedo ayudar será con gusto o de otro lado puede apoyarse directamente con la Ing Paola, quizá sea de mas ayuda.

Cordialmente,

GESTIÓN DE ADMISIONES REGISTRO Y CONTROL ACADÉMICO
ESCUELA TECNOLÓGICA INSTITUTO TÉCNICO CENTRAL

Finalmente se escala la misma pregunta a la Profesional Especializada de BD.

La Ing. Nitza Paola, en comunicación vía Teams me informa que el Software Académico Academusoft, de los cuales cuenta con la base de datos de los estudiantes de Programas de Educación Superior y respectivamente de estudiantes del Centro de Extensión y Proyección Social, así como todas sedes de la ETITC, lleva más de seis años sin adquirir soporte técnico debido a que este software no cuenta con renovación actual.

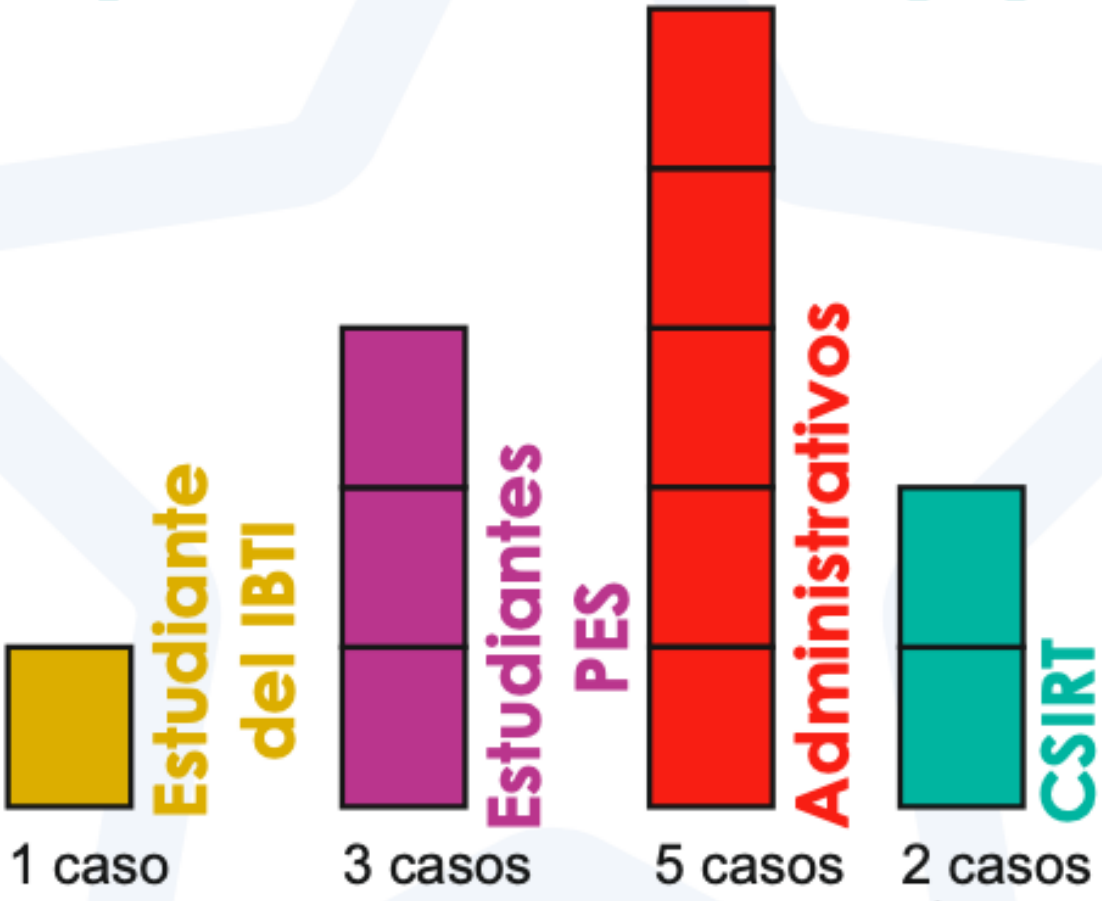
Riesgos de no tener un certificado SSL

- Visualización de advertencias en los motores de búsqueda
- Provocar la filtración a la base de datos
- Ataques MITM: (Man in the Middle) es un tipo de ataque en el que un atacante crea interferencia entre dos extremos (servidor

#3

Liderar el proceso de gestión de incidentes de seguridad, así como la posterior investigación de dichos eventos, con el fin de determinar las causas, posibles responsables y recomendaciones de mejora para los sistemas afectados, de acuerdo con los procedimientos establecidos.

Desde el 20 de Septiembre de 2021, se han reportado 11 incidentes de tipo phishing:



Incidentes ETITC

Se realiza informe con las causas, la solución y acciones realizadas y se realiza seguimiento. Se cierra el caso con el envío de la encuesta de satisfacción.

Incidentes CSIRT

Se realiza alertas y se comunica mediante correo institucional

#4

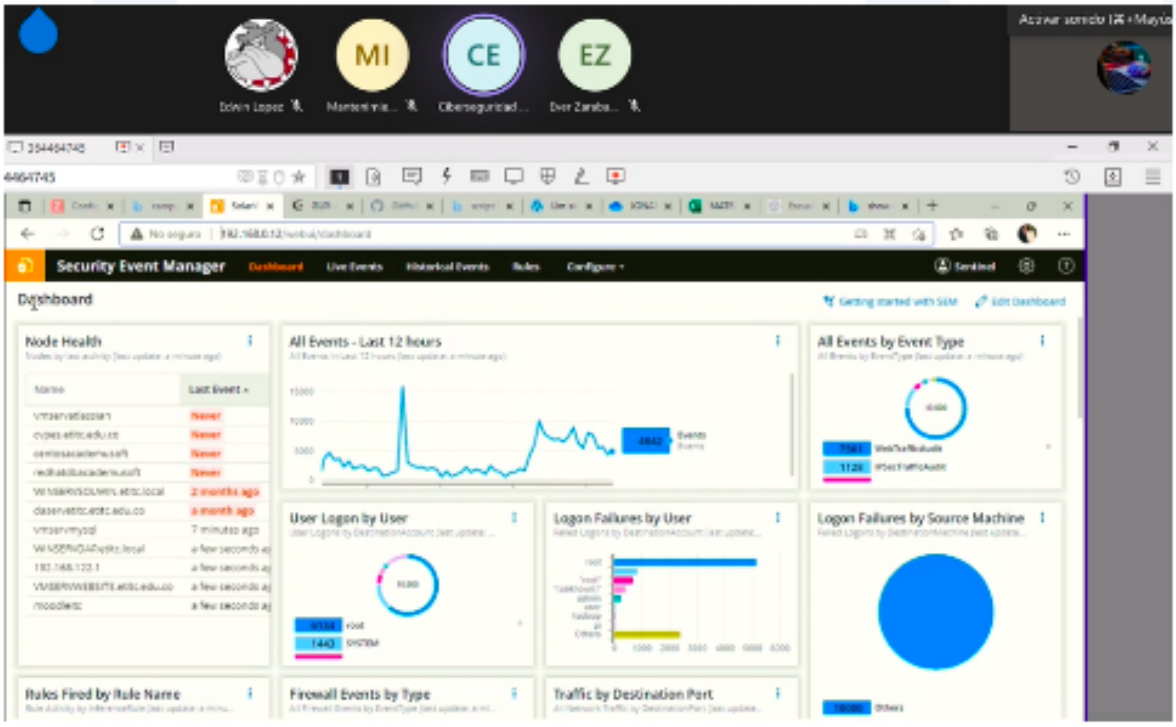
Implementar herramientas de monitoreo y correlación de eventos de seguridad de la información, de acuerdo con el modelo de seguridad y privacidad de la información del estado colombiano.

La ETITC: cuenta con 50 licencias de la herramienta SEM, en este momento se encuentran protegiendo 11 servidores de Datacenter.

- Desde el 24 de Septiembre se han recibido 13 horas de entrenamiento y monitoreo para el correlacionamiento de eventos de seguridad de la información a los servidores conectados para el Profesional de SGSI de la ETITC.

- El día 26 de Octubre se realizó la primer transferencia de conocimientos de dos horas, para los Ingenieros del área de Gestión de Informática y Comunicaciones entre ellos: Ing. Edwin López, Ing. Ever Zarabanda, Ing. Jonatan Ausique.

- El día 05 de Noviembre se culminó la transferencia de conocimientos de la herramienta SEM.



#5

Fortalecer el talento humano a través de la formación y capacitación en la cultura de seguridad de la información, de acuerdo a las Políticas, las principales amenazas y los posibles riesgos en la prestación de los servicios de la entidad.

El área de Gestión de Seguridad de la Información durante el año socializó en diversas capacitaciones la importancia del Contexto de la SI, Ciberseguridad y Seguridad Digital: Ataques Informáticos, Gestión de Contraseñas y Seguridad en la Nube.

Contexto de la Seguridad de la Información	1. Socialización de la Política de Gobierno Digital (10 de Septiembre de 2021 - Impartida por Función Pública). 2. Socialización del Sistema de Gestión de Seguridad de la Información de la ETITC (22 de Octubre de 2021 - Impartida por el profesional de Seguridad Digital para Docentes, Estudiantes de Programas de Educación Superior y Administrativos). 3. Socialización del Sistema de Gestión de Seguridad de la Información de la ETITC (11 de Noviembre de 2021 - Impartida por el profesional de Seguridad Digital para el área de Vicerrectoría de Investigación, Extensión y Transferencia).	Divulgar la Política de Operación de la Seguridad de la Información dentro del marco de la Política de Gobierno Digital del MINTIC y conocer el compromiso que el área de Seguridad de la Información fomenta estrategias para la protección de todos los activos de información de la institución en conjunto con los datos personales de toda la comunidad bajo los criterios de confidencialidad, integridad y disponibilidad.
Ciberseguridad	1. Capacitación en Webinar (22 de Julio y 12 de Agosto de 2021 - Impartida por la ESAP para las entidades púbicas y privadas). 2. Capacitación en Riesgo Informático en tendencias de Ciberataques (23 de Septiembre de 2021 - Impartida por MINTIC y FORTINET para las entidades púbicas y privadas). 3. Socialización en el primer Cyberday de Ciberseguridad (11 y 15 de Octubre de 2021 - Impartida por profesional de Seguridad Digital para Estudiantes del Instituto deBachillerato Tecnico Industrial). 4. Socialización en el primer Cyberday de Ciberseguridad (22 de Octubre de 2021 - Impartida por el profesional de Seguridad Digital para Docentes, Estudiantes de Programas de Educación Superior y Administrativos). 5. Socialización en el primer Cyberday de Ciberseguridad (11 de Noviembre de 2021 - Impartida por el profesional de Seguridad Digital para el área de Vicerrectoría de Investigación, Extensión y Transferencia).	Comprender los conceptos fundamentales de la Ciberseguridad y su enfásis es el de defender el ciberespacio de los ciberataques y garantizar que se alcancen y mantengan los objetivos del SGSI de la ETITC
Seguridad Digital: Ataques informáticos, Gestión de Contraseñas y Seguridad de la Nube	1. Socialización del Segundo Foro de Informática Forense (02 de Septiembre de 2021 - Impartida por Superintendencia de Industria y Comercio). 2. Socialización de Seguridad Digital: Ataques informáticos, Gestión de Contraseñas y Seguridad de la Nube en el primer Cyberday de Ciberseguridad (22 de Octubre de 2021 - Impartida por el profesional de Seguridad Digital para Docentes, Estudiantes de Programas de Educación Superior y Administrativos).	Socializar los lineamientos contenidas en nuestro Manual de Políticas de Seguridad y Privacidad de la Información; así mismo capacitar a nuestros estudiantes, docentes y administrativos acerca de los ataques informáticos cómo actuamos ante un phishing, malware entre otros ataques y cuál es el proceso para la prevención de los mismos. A su vez enseñar tips de seguridad para la correcta creación de contraseñas y recomendaciones en Seguridad de la nube.

Generación de contenido

Sistema de Gestión de Seguridad de la Información

Inclusión de consecutivos en los Boletínes emitidos.

Adaptación de piezas comunicativas

Creación de espacio en el sitio web informativo

Boletines Gestión de Seguridad de la Información

Ver Boletín No. 1 2021

Desarrollar el primer boletín del SGSI

Estudios Previos

El área de Planeación revisó y aprobó, el estudio previo de análisis de vulnerabilidades que se requiere dar cumplimiento con los 112 controles de seguridad de la información. Se debe contar con una firma de servicios especializados externos para el desarrollo de actividades de Pentesting y de Ethical Hacking.

Está actividad aporta mayor valor en cuestiones de auditoria de seguridad técnica, su objetivo es la revisión de controles de seguridad a los sistemas de información, así como la de los activos de información, haciendo uso de las técnicas más vanguardistas en hacking, el uso y desarrollo de los últimos exploits contra las últimas vulnerabilidades publicadas o encontrando nuevos vectores de ataques informáticos.

Informe de Gestión 2021
Gestión de Seguridad de la Información

Diagramación: Ing. Sandra J. Guerrero G.
Noviembre 24 de 2021