COMITÉ DE SEGURIDAD DE LA INFORMACIÓN 2021-3	
FECHA	**27 de octubre de 2021**

INTEGRANTES		
NOMBRE	**CARGO**	**FIRMA**
Oscar Yovany Baquero Moreno	Vicepresidente de Operaciones y Tecnología	Firmado digitalmente por BAQUERO MORENO OSCAR YOVANY Fecha: 2021.12.10 10:48:08 -05'00'
Margareth Sofía Silva Montaña	Secretaría General	
Luis Ariel Prieto Lemus	Director de Tecnología	
Carlos Javier Rodríguez	Jefe Oficina de Control Interno	
Deisy Yolima Marcelo Forero	Jefe Oficina de Riesgos	

INVITADOS	
NOMBRE	**CARGO- DEPENDENCIA /ENTIDAD**
Mauricio Cajicá Martínez	Coordinador de Infraestructura – Dirección de Tecnología
Claudia Stella Cortés Albornoz	Analista – Oficina de Riesgos
Luis Alvaro Velasquez	Contratista de seguridad - Oficina de Riesgos
Nidia Nayibe González Pinzón	Contratista de seguridad - Oficina de Riesgos
Juan de Jesús Aponte Buitrago	Contratista de seguridad - Oficina de Riesgos

AGENDA

1. Verificación del Quorum
2. Objetivos
3. Gestión de activos de información
4. Acuerdos estratégicos
5. Mejoras al SGSD (Sistema de Gestión de Seguridad Digital)
6. Avance de capacitación
7. Conclusiones

DOCUMENTOS INTEGRALES

- Presentación Comité de Seguridad de la Información de fecha 27 de octubre de 2021.
- Acta del Comité del 22 de julio de 2021

DESARROLLO

1. Verificación del Quórum

El Señor Presidente no puede asistir al Comité de Seguridad de la Información, de acuerdo con la Resolución 0460 del 20 de junio de 2013, referente a reorganización del Comité de Seguridad de la Información, el Presidente del Icetex o quien él delegue será la persona que presidirá el Comité con voz y voto; en esta línea, el Señor Presidente delega al Vicepresidente de Operaciones y Tecnología el día 26 de octubre, acción registrada en correo electrónico. Para el comité, se verifica el establecimiento del quórumpara sesionar y decidir válidamente.

El acta del comité anterior se remitió a los miembros para sus comentarios, no se recibieron observaciones; en consecuencia, se apruebael Acta del Comité de Seguridad de la Información celebrado el 22 de julio de 2021.

El Jefe de Riesgos realiza introducción del Comité y otorga la palabra a Claudia Stella Cortés, quien conjuntamente con Nidia Nayibe Gonzalez,Juan de Jesús Aponte y Luis Alvaro Velasquez realizan la exposición del Comité.

2. Objetivos

Se informa los objetivos del Comité:

- Presentar el resultado de actualización del inventario de activos de información de la Entidad, instrumento fundamental que nos lleva a identificar su clasificación, criticidad y que sirve de base para la gestión de riesgos.
- Informar la revisión realizada a las principales normas de seguridad digital, estableciendo su nivel de implementación, fortalezas y oportunidades de mejora.
- Presentar la gestión de seguridad digital en los acuerdos estratégicos, apoyando las soluciones a las necesidades institucionales

3. Gestión de activos de información

Juan de Jesús Aponte nos recuerda que es un activo de información, siendo todo aquello que genera, procesa y/o almacena la información necesaria para la operación y el cumplimiento de los objetivos de la Entidad. Además, indica los hitos principales del proceso de Inventario y Clasificación de Activos de Información que se han desarrollado en el año 2021, para todos los procesos de la Entidad:

Diagnóstico	Inventario	Clasificación	Instrumentos de Gestión
• Revisión de metodología • Revisión de normativa • Organización para la actualización de activos.	• Identificación de los activos • Definición de propietarios, responsables y custodios de los activos.	• Valoración de los activos en su confidencialidad, integridad, disponibilidad y privacidad • Aprobación del Líder del Proceso. • Consolidación. • Reporte.	• Validación de la clasificación en aspectos legales. • Generación de instrumentos de gestión. • Participación ciudadana • Divulgación en el Portal Web.

La clasificación de los activos de información se realizó de acuerdo con Ley 1712/2014 – Ley de

transparencia y acceso a la información. El hito referente a instrumentos de gestión se desarrollará entre los meses de noviembre y diciembre.

Los resultados obtenidos en el inventario y clasificación de los activos de información son:

TIPO DE ACTIVOS	CANTIDAD	PÚBLICOS	PÚBLICOS CLASIFICADOS	PÚBLICOS RESERVADOS
Sistemas de información	23		9	14
Hardware	40		32	8
Servicios	63		31	32
Programas, aplicativos, conexión software externos	83	9	49	25
Instalaciones	7		3	4
Personas	35		16	19
Información	352	53	93	206
Total	603	62	233	308

Los activos tipo información se clasificaron así:

Información Pública = 53 activos	**Información Pública Clasificada = 93 activos**	**Información Pública Reservada = 206 activos**
Toda información en posesión, bajo control o custodia de un sujeto obligado es pública y no podrá ser reservada o limitada sino por disposición constitucional o legal	Es toda información cuya divulgación debe ser rechazada, porque puede causar un daño, caso, el derecho de toda persona a la intimidad.	Es toda información cuya divulgación podrá ser rechazada, siempre que dicho acceso estuviese expresamente prohibido por una norma legal o constitucional. La reserva es temporal.

En complemento, se identificaron los activos de información más críticos de la Entidad, que tienen las características de calificación alta o crítica en confidencialidad, integridad y disponibilidad, ellos son 114 activos, los cuales son revisados desde gestión de riesgos de seguridad digital para determinar su adecuada protección.

El Jefe de la Oficina de Control Interno menciona que aunque no sea directo del numeral expuesto, se continúa identificando en las auditorías realizadas en las Oficinas de Icetex (CEP's) que el personal del Proveedor de Atención al cliente se comparte claves de acceso, Claudia Cortés aclara que esta situación no debería ocurrir porque el proceso de gestión de acceso a los sistemas de información es ejecutado diariamente y todo lo recibido por la herramienta de gestión se atiende, además que existe un monitoreo periódico, por cuanto volverá a revisar el tema con la Oficina de Comercial y Mercadeo.

4. Revisión del SGSD

Luis Alvaro Velasquez informa que se ha revisado las siguientes normas de seguridad de la información que Icetex debe atender:

4.1. Estándar ISO 27001

La Norma ISO 27001 es la norma definida por MinTic para gestionar la seguridad de la información en las

entidades públicas, por ello la Oficina de Riesgos realiza la revisión de su cumplimiento.

La norma la conforman 114 controles, que se encuentran clasificados por temas, a los que se denomina "Dominios", cuyos resultados son:

Numeral	Dominio	Calificación
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	96
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	100
A.8	GESTIÓN DE ACTIVOS	98
A.9	CONTROL DE ACCESO	98
A.10	CRIPTOGRAFÍA	100
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	97
A.12	SEGURIDAD DE LAS OPERACIONES	90
A.13	SEGURIDAD DE LAS COMUNICACIONES	100
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	86
A.15	RELACIONES CON LOS PROVEEDORES	90
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	99
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	100
A.18	CUMPLIMIENTO	96,5
PROMEDIO EVALUACIÓN DE CONTROLES		**96**

El cumplimiento de la norma ISO27001:2013 es del 96%, identificando las siguientes fortalezas y oportunidades de mejora:

Fortalezas:

- El sistema se monitorea para el cumplimiento de los procedimientos y tomar medidas de acción frente a debilidades.
- La implementación de los controles de la ISO27001, incorporados en la operación de la Entidad.
- Inversiones en tecnologías de seguridad de la información y ciberseguridad.

Oportunidades de mejora:

Oportunidades de mejora	Responsable
A.8.2.2 Fortalecer la gestión de activos de información Reforzar el etiquetado de documentos de acuerdo con los niveles de clasificación.	O. Riesgos
A.14.2.2 Fortalecer el desarrollo y mantenimiento de sistemas • A.14.2.2 Gestionar lista de chequeo de seguridad para desarrollo de software • A.14.3.1 Anonimizar los datos para pruebas	D. Tecnología
A.18.1.2 Documentar procedimiento para el cumplimiento de requisitos de propiedad intelectual y software patentado	O. Riesgos / D. Tecnología

4.2 Normas de la Superfinanciera

4.2.1 Circular 029-2014 - Canales, medios, seguridad y calidad en el manejo de información de prestación de servicios financieros, la seguridad y calidad para la realización de operaciones

El informe de la Circular Básica Jurídica 029 de 2014 Parte 1, Título II, Capítulo I – Canales, medios, seguridad y calidad en el manejo de información de prestación de servicios financieros de la Superintendencia Financiera de Colombia, contiene la revisión y oportunidades de mejora para fortalecer la gestión de seguridad de la información y a ciberseguridad. La Circular contiene 150 controles que aplican al Icetex 88, por las operaciones y servicios que se realizan.

El Cumplimiento de Circular es del 93% identificando las siguientes fortalezas y oportunidades de mejora:

Fortalezas:

- Los servicios para la transferencia segura de información
- Gestión de proveedores
- Capacitaciones
- Mejor uso de las herramientas tecnológicas para la protección información

Oportunidades de mejora

Oportunidades de mejora	Responsable
2.3.4.9.5. Informar al cliente, al inicio de cada sesión, la fecha y hora del último ingreso a este canal.	D. Tecnología
2.3.3.1.22. Informar sobre la disponibilidad de cada uno de los canales por medio de los cuales presta sus servicios.	D. Tecnología
2.3.4.10. Avisar la prestación de servicios a través de nuevos canales.	OCM
2.3.3.2.6. Llevar un registro de las consultas realizadas por los funcionarios de la entidad sobre la información confidencial de los clientes.	D. Tecnología

4.2.2 Circular Externa 007 de 2018 - Requerimientos mínimos para la gestión de la seguridad de la información y la ciberseguridad

La Circular de Ciberseguridad contiene 49 controles que aplican todos al Icetex y el nivel de cumplimiento es del 97% identificando las siguientes fortalezas y oportunidades de mejora:

Fortalezas:

- Trabajo articulado con grupos de interés como la Dirección Nacional de Inteligencia DNI y la Superfinanciera.
- Capacidades de alertar y reaccionar ante amenazas cibernéticas.
- Implementado el reporte de métricas de seguridad de la información y ciberseguridad.

Oportunidades de mejora

Oportunidades de mejora	Responsable

3.8 Incluir dentro del ciclo de vida del desarrollo del software, incluyendo servicios web y apps, que procesan la información confidencial de la entidad aspectos relativos con la seguridad de la información que permitan mitigar		dicho riesgo. Complementar la lista de verificación de controles para el desarrollo desoftware

3.3 Contar con un sistema de gestión para la ciberseguridad, para lo cual se pueden tomar como referencia el estándar ISO 27032.	Oficina de Riesgos
3.6 Establecer procedimientos para la retención y destrucción final de la información. Se encuentra en implementación la Política de preservación digital a largo plazo	Dirección de Tecnología Grupo de Gestión Documental Oficina de Riesgos

En complemento, se informa que se entregó el 10 de octubre a la SFC – Reporte de F408 de métricas e incidentes - Circular 033 de 2020.

4.2.3 Circular Externa 005 de 2019 - Reglas relativas al uso de servicios de computación en la nube

La Circular de Nube contiene 34 controles que aplican todos al Icetex y el nivel de cumplimiento es del 93% identificando las siguientes fortalezas y oportunidades de mejora:

Fortalezas:

- Exigencia de disponibilidad de al menos el 99.95% en los servicios prestados en la nube.
- Garantizar la independencia de su información y de sus copias de respaldo de la información de las otras entidades que procesen en la nube.
- Tener bajo nuestro control la administración de usuarios y de privilegios para el acceso a los servicios ofrecidos.

Oportunidades de mejora

Oportunidades de mejora	Responsable
3.16 Establecer las medidas necesarias para garantizar que, en el evento de toma de posesión, la SFC, pueda acceder a la información y a la administración de los sistemas de información que operan en la nube.	Dirección de Tecnología
6. Remisión de la información a la SFC dentro de los 15 días anteriores al inicio del procesamiento de información en la nube, relacionada con procesos misionales o de gestión contable y financiera.	Dirección de Tecnología
7.3 Las entidades deben mantener actualizada y a disposición permanente de la SFC, la documentación de los flujos de datos de los procesos misionales o de gestión contable y financiera que alimentan o consumen las aplicaciones dispuestas por el proveedor de servicios en la nube.	Dirección de Tecnología

Es de anotar que este informe tiene un sustento documental y se está desarrollando los planes de acción.

El Vicepresidente de Operaciones y Tecnología solicita se establezcan y desarrollen los planes de acción

sobre los temas a fortalecer en las normas revisadas.

5. Acuerdos Estratégicos

Claudia Cortés informa que la Oficina de Riesgos participa en la revisión de las propuestas de Acuerdos Estratégicos según los lineamientos generales de las Políticas de celebración y ejecución de acuerdos

estratégicos, a la fecha se han revisado 28 propuestas de Acuerdos Estratégicos, efectuando el siguiente análisis de seguridad digital:

- Revisión del documento previo y generando concepto.
- Revisión de la matriz de riesgos de contratación.
- Apoyo en el intercambio de información.
- Revisión del convenio cuando es requerido.

6. Mejoras al SGSD

Claudia Cortés informa que se ha creado el Instrumento de seguimiento del Sistema de Gestión Seguridad Digital, que busca una mayor apropiación de sistema por los colaboradores y mejorar su administración.

- El instrumento está conformado por los principales aspectos transversales del SGSD: revisión de usuarios, almacenamiento de información y etiquetado, seguimiento de responsabilidades de proveedores, revisión de autorización de tratamiento de datos personales y matriz de riesgos.
- Este documento será de atención por parte de todas las áreas.
- La frecuencia de reporte es trimestral.

7. Avances en Capacitación

Nidia Nayibe Gonzalez expone los avances en capacitación:

7. 1. Capacitaciones internas

- La reinducción tiene un avance del 98,24% del total de la población del ICETEX capacitados en Seguridad Digital.
- Se capacitó por solicitud a la Dirección de Tesorería y Grupo de Crédito en los siguientes temas:
  - ✓ Inventario de Activos de Información
  - ✓ Etiquetado de Información
- Se implementó Capacitación de Etiquetado, que se encuentra alojado en el SharePoint de Talento Humano.
- Se ha venido avanzando con la sensibilización e implementación del Múltiple factor de Autenticación en la Vicepresidencia de Operaciones y Tecnología y Secretaría General.

7.2. Capacitación al Proveedor de Atención al Cliente

Se elabora capacitación específica para el Proveedor de Atención al Cliente en virtud de la cantidad de colaboradores y el múltiple uso de la información de la Entidad. En la capacitación se suministran los siguientes temas:

- Políticas de seguridad Digital
- Conceptos de Ciberseguridad:
  - ✓ Ciberseguridad
  - ✓ Phishing
  - ✓ Ramsonware
- Cuidado de la información

- Control de accesos
  - ✓ Incidentes
  - ✓ Clasificación de la información

Los responsables de esta capacitación son las áreas de Oficina Comercial y Mercadeo y Oficina de Riesgos.

7.3. Prueba de Ingeniería Social

La ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios. Se realizó prueba de ingeniería social a través de correo electrónico el 22 de septiembre a 100 colaboradores donde se solicitaba actualizar datos de contraseña. Los resultados de la prueba son los siguientes:

Alertaron y procedieron correctamente	Comprometieron información	Fueron indiferentes
24	32	44

En consecuencia, la Oficina de Riesgos procederá así:

- Felicitar a los usuarios que informaron
- Capacitación en el manejo de información a 76 usuarios

Conclusiones

- Las áreas han adelantado un ejercicio más profundo en la revisión del inventario y clasificación de activos de información y lo reconocen como instrumento para desarrollar los controles de seguridad de la información.
- Las áreas han adelantado un ejercicio más profundo en la revisión del inventario y clasificación de activos de información y lo reconocen como instrumento para desarrollar los controles de seguridad de la información.
- El sistema de gestión de seguridad digital se desarrolla basado en las normas existentes en la materia y en su ejecución, por lo que es necesario hacer las revisiones periódicas para establecer fortalezas como también debilidades que podrían llevarnos a incidentes.
- Los acuerdos estratégicos se deben desarrollar garantizando la protección de la información de la Entidad y de los aliados.

El Ingeniero Oscar Baquero, quien preside este Comité de seguridad de la Información, agradece el trabajo realizado y hace un reconocimiento al trabajo en equipo construido entre la Dirección de Tecnología, la Oficina de Riesgos y Secretaria General y menciona que seguramente si el señor Presidente estuviese resaltaría el trabajo destacado y los logros obtenidos.

La Jefe de la Oficina de Riegos agradece al Vicepresidente por haber presidido el comité, al equipo de

seguridad digital y a todos por la participación del comité en el día de hoy.

CONSTANCIAS Y COMPROMISOS DEL ACTA

No.	Compromiso	Responsable	Fecha Inicio	Fecha Fin	Observación
1	Definición de planes de acción sobre las oportunidades de mejora de las normas de seguridad revisadas	Oficina de Riesgos Dirección de Tecnología	01/11/2021	15/12/2021	

Elaboró: Claudia Stella Cortés Albornoz – Analista de Riesgos

Revisó: Monica Pinto Garcia – Coordinadora de Riesgos No Financieros