

**INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO  
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS  
ESPECIALIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN**

**IMPLEMENTACIÓN DE SOLUCIONES EN UNA INSTITUCIÓN UNIVERSITARIA  
PARA MITIGAR LA PÉRDIDA Y/O ALTERACIÓN DE LA INFORMACIÓN POR  
FALENCIAS EN LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN Y  
SEGURIDAD FÍSICA.**

**PRESENTA:  
ANGIE KATHERINE BOHÓRQUEZ RODRÍGUEZ  
Cod. 1612011063**

**ASESOR TEMÁTICO:  
WILMAR JAIMES FERNÁNDEZ  
PTC TITULAR**

**MAYO 2018**

## ÍNDICE GENERAL

RESUMEN.....	4
PALABRAS CLAVE.....	6
INTRODUCCIÓN.....	7
ESTADO DEL ARTE.....	9
ESTRATEGIA METODOLÓGICA.....	16
DESARROLLO E IMPLEMENTACIÓN .....	18
RESULTADOS .....	25
DISCUSIÓN Y CONCLUSIONES.....	27
REFERENCIAS .....	28

## ÍNDICE DE FIGURAS

Ilustración 1 - Sede 1 antes.....	10
Ilustración 2 - Sede 1 proyectada a 3 años .....	10
Ilustración 3 - Sede 2.....	11
Ilustración 4 - Sede 3.....	11
Ilustración 5 - Sede 3 con construcción y parqueadero a lado y lado .....	12
Ilustración 6 - Sede 4.....	12
Ilustración 7 - Sede 5.....	13
Ilustración 8 - Sede 6.....	13
Ilustración 9 - Sede 7.....	14
Ilustración 10 - App Alissta.....	20
Ilustración 11 – Pieza divulgación cambio de clave.....	23

## **RESUMEN**

En la Institución Universitaria en estudio, actualmente se observa que la cantidad de estudiantes está creciendo significativamente, tanto de modalidad presencial como de modalidad virtual, por lo que la impartición de clases hoy en día es una necesidad de primera mano puesto que es el core de la Institución. Lo anterior, obliga a generar espacios adecuados para dictar las diferentes cátedras que se imparten, por lo que los altos directivos de la Institución tomaron la decisión de derrumbar uno de sus edificios, el más antiguo, para así poder construir uno que se ajuste a las necesidades del crecimiento estudiantil y al nivel de la misma, para seguir entregando una buena educación acorde a las necesidades del entorno.

En vista de la demolición del anterior edificio y la construcción del nuevo, se están empezando a observar diferentes inconvenientes por el traslado de salones a otras sedes, hacinamiento del personal contratado, incidentes en infraestructura física, problemas de seguridad que están empezando a ocasionar pérdidas y/o alteraciones de la información, y un sin número de actividades negativas que traen consigo los anteriores inconvenientes mencionados.

Es por esto, que se realizará un apoyo a la persona encargada en la Institución de sacar adelante todo lo correspondiente de la Seguridad de la Información, lo cual acoge toda la parte física y lógica de toda la infraestructura de la Institución, para así lograr corregir o minimizar los inconvenientes de seguridad física y seguridad de la información; dichas soluciones pueden ir desde la contratación de una empresa de vigilancia idónea hasta sistemas de controles de acceso para la parte física, además de la elaboración y puesta en marcha de políticas y manuales de seguridad de la información dentro y fuera de la infraestructura física de la Institución, con lo cual se logrará tener un mejor control de los incidentes que se puedan presentar por fallas en la seguridad física o lógica y que se puedan materializar en la Institución Universitaria, permitiendo consigo tener un parte satisfactorio de tranquilidad encaminado a un correcto crecimiento tanto interno como externo de la academia.

## **ABSTRACT**

In the University Institution under study, it is currently observed that the number of students is growing significantly, both in face-to-face modality and virtual modality, so the teaching of classes today is a necessity first hand since it is the core of the institution. The foregoing, forces to generate spaces chords to dictate the different chairs that are taught, reason why the high managers of the Institution took the decision to demolish one of their buildings, the oldest, in order to be able to build one that adjusts to the needs of student growth and the level of it, to continue delivering a good education according to the needs of the environment.

In view of the demolition of the previous building and the construction of the new one, different inconveniences are beginning to be observed due to the transfer of halls to other locations, overcrowding of contracted personnel, incidents in physical infrastructure, security problems that are beginning to cause losses and / or alterations of the information, and a number of negative activities that bring with them the aforementioned drawbacks.

For this reason, a small consultancy will be carried out, supporting the person in charge of the Institution to carry out all the corresponding Information Security, which includes all the physical and logical part of the Institution's entire infrastructure, to correct or minimize the drawbacks of physical security and information security; These solutions can range from the hiring of a suitable surveillance company to access control systems for the physical part, as well as the elaboration and implementation of information security policies and manuals inside and outside the physical infrastructure of the Institution, with which it will be possible to have a better control of the incidents that may occur due to failures in the physical or logical security and that may materialize in the University Institution, allowing to have a satisfactory part of tranquility aimed at a correct growth both internal as well as external to the academy

## **PALABRAS CLAVE**

Seguridad y salud en el trabajo: Consiste en el desarrollo de un proceso lógico y por etapas, basado en la mejora continua y que incluye la política, la organización, la planificación, la aplicación, la evaluación, la auditoría y las acciones de mejora con el objetivo de anticipar, reconocer, evaluar y controlar los riesgos que puedan afectar la seguridad y salud en el trabajo. [1]

Manual de seguridad de la información: Documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI (Sistema de Gestión de la Seguridad de la Información) [2]

## **INTRODUCCIÓN**

El problema a tratar directamente es la pérdida y/o alteración de información ya sea de la academia o de la parte administrativa, por los robos o alteración de la misma por los robos presentados de equipos de cómputo o documentos físicos, o por las fallas de políticas de seguridad informática que no permiten el correcto salvaguardo de la información basado en la triada CIA, además de constantes problemas en la seguridad física de todas las sedes de la Institución Universitaria por inconvenientes de la infraestructura tecnológica y física.

Este es un problema que con el pasar de los días va creciendo puesto que, a partir del comienzo del año 2018 la Institución fue dividida un total de 7 sedes debido a la distribución que se tuvo que realizar por la demolición del edificio antiguo y la construcción del nuevo lo cual asegurará dentro de tres años el correcto funcionamiento de la Institución con el crecimiento de estudiantes proyectado, además, el hecho de tener que arrendar 3 de las sedes no permite la fácil adecuación de las mismas de acuerdo a las necesidades que se presenten y en el momento en el que se presenten puesto que para realizar modificaciones o reparaciones se debe solicitar la autorización del dueño lo cual perjudica en tiempo de solución. El principal inconveniente en estas tres sedes arrendadas es la falta de sistemas de control acceso para permitir el ingreso de las personas autorizadas como lo son estudiantes, empleados, docentes y directivos, al igual que el personal de los proveedores que se tienen contratados para brindar servicio dentro de la Institución, dicha ausencia del control de acceso se ha visto notablemente reflejada en robos de equipos portátiles lo que asegura un manejo no autorizado información allí alojada que es el activo más importante de la Institución, así como pérdida de activos materiales que también cuestan.

Así mismo, se han detectado incidentes a nivel de seguridad lógica en cuanto a permisos sobre carpetas red, correo electrónico, virus, lo que afecta notablemente la información que se tenga almacenada digitalmente puesto que en ocasiones es alterada o eliminada. Dichas alteraciones o pérdidas de información, también pueden estar asociadas a ambientes laborales poco idóneos lo que trae consigo empleados no satisfechos, generando mal ambiente ocasionado por problemas de hacinamiento en las sedes que alojan personal administrativo, o por sedes ya muy viejas con múltiples problemas de tipo estructural afectando la salud en el trabajo, por ejemplo, una de las sedes que si es propia, pero que al ser una edificación muy vieja y patrimonio nacional, ya tiene serios problemas que no se pueden intervenir al 100% puesto que por ser patrimonio nacional no se puede realizar ningún tipo de modificación de infraestructura, por lo cual, cada vez que falla algo o hay algún tipo

de daño se subsana de la mejor manera pero de manera correctiva, es decir cuando ya se ha habido serios daños a nivel de cualquier activo, y para el enfoque de la consultoría a nivel tecnológico puesto que ya se han dañado computadores por diferentes inundaciones dentro de la sede, perdiendo así información que altera el normal desarrollo de actividades o cuando se han detectado riesgos inminentes que afecten a las personas que trabajan o visitan la sede.

Por lo anterior, los objetivos de éste estudio son:

- Principal: Minimizar los incidentes presentados de pérdida o alteración de información de la Institución Educativa
- Específicos:
  - ✓ Detectar los problemas de infraestructura y seguridad física de la Institución que puedan llegar a alterar la información
  - ✓ Implementar políticas de seguridad de la información que permitan salvaguardarla correctamente
  - ✓ Concientizar a los empleados, docentes y estudiantes sobre la importancia de la seguridad dentro de la Institución



## **ESTADO DEL ARTE**

En cualquier institución o empresa, la seguridad física debe ir relacionada con la seguridad de la información para así prevenir fugas y pérdida de información, es por esto, que a continuación se evidenciará lo que se debe asegurar en cualquier empresa o institución para un correcto manejo de seguridad en general.

### Seguridad física:

Se entiende que es todo lo que pueda poner en riesgo, sea cual sea su impacto, a los activos más importantes de la compañía como lo son la información y el recurso humano, que permitan proteger todos los recursos físicos de la compañía.

Los objetivos principales de esta seguridad son los siguientes:

- Entender la importancia que tiene la seguridad física dentro las organizaciones con el fin de brindar actividades de prevención y ante cualquier evento.
- Identificar los componentes que están asociados con la seguridad física y como es su interacción en la protección de los activos físicos.
- Aplicar los conocimientos adquiridos en el análisis de ejercicios de aplicación en donde las necesidades de las empresas varían de acuerdo a lo que quieren salvaguardar.
- Comprender la importancia de tener un plan de seguridad en donde se contemplen todos los factores que está directamente involucrados con la seguridad física, y así realizar su respectivo análisis y toma de decisiones [3]

En la protección de los recursos físicos de la compañía, se deben tener en cuenta los problemas a los que se encuentra expuesta como lo son: acceso físico, desastres naturales, alteraciones del entorno y factores humanos.

Para el caso de la Institución Universitaria en estudio, se tiene que tienen varias sedes las cuales están distribuidas así:

- Sede 1: En el sitio de la construcción del nuevo edificio, lo que puede permitir el acceso no autorizado de personal a la sede por medio de las puertas de los encargados de la construcción. Dicha sede cuenta con un sistema de talanqueras con lector de carnet y huella digital para permitir el ingreso de las personas registradas como empleados y estudiantes de la Institución, para los visitantes se tiene el procedimiento de registro en recepción dejando un documento y haciendo entrega de una tarjeta de visitante que permita el

acceso por talanquera. Ésta sede tiene todos los salones físicos para clases presenciales y la Biblioteca de la Institución.



*Ilustración 1 - Sede 1 antes*



*Ilustración 2 - Sede 1 proyectada a 3 años*

- Sede 2: Ubicada en frente a la Sede 1, arrendada mientras el tiempo de construcción del edificio nuevo, con un vigilante a la entrada, pero sin un sistema de control de acceso. Allí se encuentran procesos importantes como lo son la Tesorería y Registro Académico, además del proceso de Admisión a la Institución.



*Ilustración 3 - Sede 2*

- Sede 3: Ubicada igualmente al frente de la Sede 1 de manera diagonal en la esquina, en la cual se encuentran todos los decanos y asistentes de las diferentes facultades, incluyendo los docentes de planta sin puesto fijo, es rotativo. Arrendada, con un vigilante a la entrada, pero igualmente que la Sede 2, sin un sistema de control de acceso. Este edificio es de 3 pisos y actualmente presenta fallas de estructura puesto que, al ser esquinero, sólo tiene un apoyo con otra construcción puesto que, del otro lado, se está realizando una obra hace más de 1 año, lo que está ocasionando inestabilidad de la infraestructura y deterioro por agrietamiento.

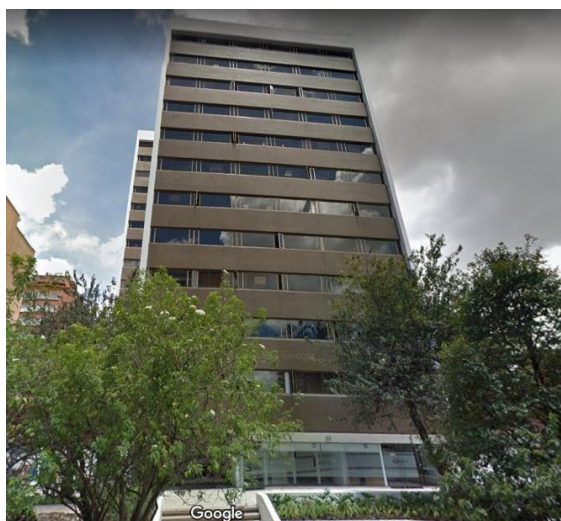


*Ilustración 4 - Sede 3*



*Ilustración 5 - Sede 3 con construcción y parqueadero a lado y lado*

- Sede 4: Ubicada en un edificio en los pisos 4 y 5, allí se encuentra ya la gran mayoría de procesos administrativos de la Institución como lo son: Contabilidad, Tecnología, Comunicaciones, Planeación, Desarrollo Humano, Presupuesto. Son dos pisos arrendados en el edificio que aloja a más de una empresa, sólo tiene acceso por talanquera para las personas que entren con carnet dispuesto por la administración del edificio, pero cualquier persona puede ingresar a los pisos de la Institución puesto que no hay ningún tipo de control sobre el acceso a las instalaciones. La vigilancia contratada sólo hace presencia a ciertas horas del día para apertura y cierre de las oficinas de lunes a sábado. Allí cada persona tiene un equipo de cómputo asignado sea portátil o desktop



*Ilustración 6 - Sede 4*

- Sede 5: Ubicada al lado de la Sede 4, es una casa arrendada que tampoco cuenta con un sistema de control de acceso, sólo la presencia de un vigilante, allí se encuentran procesos como Compras y toda la atención estudiantil orientada al Bienestar, Cultura y Deporte, Gimnasio, Salones especializados para danza, teatro y demás.



*Ilustración 7 - Sede 5*

- Sede 6: Ubicada casi a 4 cuadras de la sede 1 la cual aloja a la mayoría de laboratorios de la Facultad de Ingeniería con importantes equipos especializados para cada área del conocimiento de la facultad. Igualmente, que varias sedes anteriores, con un vigilante sin sistema de control de acceso



*Ilustración 8 - Sede 6*



- Sede 7: Ubicada a 6 cuadras de la sede 1 la cual es patrimonio nacional, propia de la Institución la cual aloja procesos como Tecnología, Facultad a distancia, salas de tutoría virtual, Gestión Comercial, Mediaciones Didácticas, Punto Vive Digital del MINTIC, con un sistema de control de acceso y vigilante permanente. Allí cada sala de tutoría cuenta con un equipo de cómputo fijo, igualmente cada colaborador cuenta con un equipo de cómputo. Actualmente esta sede presenta varios daños de estructura en techos, paredes, tuberías lo que ha ocasionado daño de equipos de cómputo.



*Ilustración 9 - Sede 7*

De acuerdo a la descripción anterior se tienen identificados los siguientes 4 principales inconvenientes en cuanto a seguridad física:

1. Débil sistema de control de acceso
2. Empresa de seguridad contratada no apta para el desarrollo de actividades en la Institución
3. Fallas de infraestructura
4. Hacinamiento de empleados

Para los problemas #3 y #4, se debe tener en cuenta todo lo dispuesto en el manual de Salud y Seguridad en el trabajo con el que debe contar la Institución para garantizar un correcto ambiente laboral y por ende la salud de sus empleados. Para esto se puede recibir toda la asesoría de la ARL que se tenga contrata para detectar

posibles riesgos laborales en cuanto a infraestructura sin dejar de lado el cómo actuar ante incidentes de tipo natural, accidentes laborales y demás.

Igualmente, se puede empezar a basar el Sistema de Salud y Seguridad en el Trabajo con la normatividad OHSAS de Icontec bajo la norma OHSAS 18001, la cual “especifica los requisitos para un sistema de gestión de Salud y Seguridad Ocupacional que le permita a una organización desarrollar e implementar una política y objetivos que tengan en cuenta los requisitos legales e información acerca de riesgos de seguridad y salud ocupacional. Se busca su aplicación a todo tipo y tamaño de organizaciones, y dar cabida a diversas condiciones geográficas, culturales y sociales” [4]

Teniendo en cuenta dichos problemas, se empata la seguridad física con la seguridad de la información, que se describe a continuación.

#### Seguridad de la Información:

De acuerdo a lo descrito en la Norma Técnica Colombiana Iso 27001, es la “preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.” [5]

Para la institución en estudio, se observa que no se tienen lineamientos sobre el manejo de la información que permita un correcto salvaguardo de la misma en el que los problemas #1 y #2 detectados en seguridad física son riesgos inminentes en cuanto a seguridad de la información, los cuales deben estar inmersos en el manual de seguridad de la información que se debe implementar en la Institución Universitaria, lo cual permite saber el impacto, las vulnerabilidades y amenazas que traen consigo, para así atacarlos e intentar minimizarlos o eliminarlos como riesgos, asegurando de manera efectiva el salvaguardo de la información de la Institución, reduciendo al máximo el acceso de personal no autorizado a cualquier sede de la Institución y a cualquier tipo de información, el robo de activos, sin dejar a un lado los riesgos de tipo natural o estructurales que puedan afectar a las diferentes sedes y por ende a la información.

## **ESTRATEGIA METODOLÓGICA**

Teniendo en cuenta que las causas de pérdida de información dentro de la Institución están asociadas a falencias en cuanto a seguridad física y seguridad lógica, se deben buscar soluciones en lo posible a corto plazo que estén avaladas por los altos mandos puesto que sin el apoyo de ellos, no se podrán realizar actividades que requieran dinero no presupuestado para el año vigente, una vez se tenga dicha aprobación se asegura que las soluciones a pesar de que afectan el flujo de caja, no alteran el normal desarrollo de todo tipo de actividad de la Institución.

Es por esto, que se deben agendar reuniones con los diferentes implicados en los procesos (áreas de la institución) relacionados con la parte de seguridad física y seguridad de la información, para poder saber qué es lo que cada uno ha detectado como incidentes y si ya han sido resueltos o no, para poder abordar y atacar los que generan un impacto mayor como prioridades e ir minimizando la brecha de inseguridad que está afectando a la información de la Institución. Una vez reunida toda la información suministrada por los procesos, ésta se debe presentar a los altos mandos para tomar la decisión de qué hacer y cómo actuar frente a cada inconveniente lo cual permitirá minimizar todo tipo de riesgo que ponga en juego la información y por ende la imagen institucional, y así poder cumplir con lo proyectado en crecimiento, misión y visión institucional.

Siendo así, y previo a la reunión con todos los procesos, se plantean buscar las soluciones a los siguientes inconvenientes:

Para la parte de seguridad física:

- Evaluar la continuidad de la empresa de vigilancia actualmente contratada o verificar si los procesos y procedimientos ejecutados por ella son los correctos para entrar a modificarlos o reestructurarlos
- Validar el estado de todas las infraestructuras de las sedes de la Institución para detectar todo tipo de riesgos para poder clasificarlos y empezar a atacar los que generen mayor impacto
- Con el apoyo de Recursos Humanos, validar los espacios físicos vs e personal contratado para detectar si las sedes contratadas actualmente son las necesarias o se requiere de otra sede o modificaciones en contratos para manejar el teletrabajo y así optimizar espacios



- Solicitar cotizaciones para la implementación del sistema de control de acceso que incluya a todas las sedes con mínimo una talanquera, un biométrico y un lector de carnet por sede para así validar las personas autorizadas para ingreso a las diferentes sedes de la Institución

Para la parte de seguridad lógica:

- Estructurar un comité de seguridad de la información (que incluye información física y lógica) para determinar los lineamientos básicos de salvaguardo de la misma
- Realizar un mantenimiento, y todas las actividades que esto conlleve, a todos los equipos de seguridad de redes tanto de hardware como de software para asegurar protección de la red interna con todas las actualizaciones necesarias para ello.

## **DESARROLLO E IMPLEMENTACIÓN**

Se realizó reunión con las coordinaciones de los procesos directamente implicados, los cuales son:

- Coordinador de Servicios Logísticos: A cargo de los proveedores contratados como tercerizados, y todo el mantenimiento de la infraestructura física de la Institución
- Coordinador de Sistemas de Información: A cargo de todo tipo de software contratado para ser usado dentro de la Institución
- Coordinador de Infraestructura: A cargo de la red y equipos tecnológicos de la Institución
- Coordinador de Datacenter: A cargo del aprovisionamiento y mantenimiento de servidores y Datacenter, actualmente es la persona encargada de las labores de seguridad de la información
- Coordinador de Secretaría General: A cargo de todos los procedimientos legales de los diferentes contratos, convenios y situaciones que se requiera dentro de la Institución. Implementador del procedimiento para el cumplimiento de la Ley de Habeas Data
- Coordinadora de Personal: A cargo de todo tipo de contratación dentro de la Institución
- Coordinadora de Salud y Seguridad en el trabajo: A cargo de todo lo relacionado con ambiente laboral y salud ocupacional de la Institución

A ellos se les planteó la situación que está generando alarma y se les expusieron los 6 problemas antes mencionados, para lo cual estuvieron totalmente de acuerdo, e indicaron que atacando estos 6 frentes se solucionan muchos inconvenientes que se presentan dentro de la Institución.

Entre las personas antes mencionadas, se acordaron las siguientes acciones a tomar como solución a dichos problemas, las cuales se describen a continuación:

1. Empresa de vigilancia: Desde Servicios logísticos con el apoyo de la Coordinadora de Secretaria General, se va a mirar el contrato actualmente suscrito con la empresa, para verificar la vigencia, las clausulas para ver si se puede realizar otrosí modificando y/o agregando términos que obliguen a la empresa a desempeñar correctamente la labor teniendo en cuenta las necesidades de la Institución. De decidir la terminación del contrato, se empezará el proceso debido de contratación para lo cual se empezarán a

solicitar ofertas a diferentes proveedores de vigilancia, para entrar a evaluar y escoger la empresa con apoyo del Vicerrector Financiero, quien da el visto bueno para el monto a cancelar del contrato pactado.

Entre las principales razones por las que se pone en tela de juicio el actuar de la empresa de vigilancia, es que se han presentado varios robos de equipos portátiles en diferentes sedes y a la hora de realizar la verificación en las cámaras no se encuentra evidencia clara que permita encontrar al responsable, o no se tiene un adecuado registro de personal no autorizado en las bitácoras (en las sedes donde no se cuenta , esto teniendo en cuenta que como se manifestó anteriormente, no todas las sedes tienen sistema de control de acceso) lo que ocasiona un alto riesgo de que personas inescrupulosas puedan alterar o usar malintencionadamente cualquier activo de la Institución con información de cualquier tipo.

Dicha revisión y decisión, actualmente está pendiente por parte de los dos procesos encargados, por diferentes actividades de cada uno que tiene a cargo, y la cual sólo la pueden tomar ellos quienes son los responsables del proceso de contratación dentro de la Institución y cumplimiento de la misma.

2. Infraestructuras de las sedes: La revisión y mantenimiento de todas las sedes, está a cargo de la Coordinación de Servicios Logísticos, quien confirma las siguientes actividades realizadas en las diferentes sedes:
  - En la sede 3 que es la más afectada actualmente, en conjunto con el dueño de la edificación ya se realizaron labores de arreglo de grietas y revisión estructural de la sede, para prevenir el movimiento constante ty brusco del edificio o un eventual y catastrófico desplome.
  - En la sede 7 se están haciendo arreglos de techos y tuberías, quienes han sufrido constantes fallas últimamente permitiendo la inundación y daño de equipos de cómputo o documentos físicos, y más en la temporada de lluvia en la que actualmente se encuentra Bogotá. También se han realizado reparaciones y cambios de cañerías, así como las actividades del día a día que permitan tener una infraestructura segura que pueda asegurar a los estudiantes, empleados y a la información de Institución.

Además, en conjunto con la Coordinación de Seguridad y Salud en el Trabajo de la Institución y la ARL Positiva, se lanzó una campaña para el reporte de

cualquier tipo de riesgo laboral por parte de cada empleado desde una aplicación a la cual se puede acceder con el número de NIT y número de documento. Dicha aplicación es revisada constantemente por la Coordinación de Seguridad y Salud en el Trabajo de la Institución, con el fin de determinar si lo reportado corresponde a una falla de infraestructura o a reportes de tipo laboral relacionados con la labor que desempeña cada empleado dentro de la institución. Para lo anterior, se envió por correo masivo a toda la comunidad de la Institución la siguiente pieza informativa:

Ahora podrás reportar riesgos laborales desde tu teléfono

Descarga la App **ALISSTA** de Positiva ARL y tendrás un canal directo de comunicación con la Coordinación de Seguridad y Salud en el Trabajo.

**'Alissta' te presta los siguientes servicios:**

<b>Comunicación:</b> Conoce tips, consejos e información actualizada del SGSST.	<b>EPP:</b> Conoce los elementos de protección personal que exige tu labor.
<b>Rendición de cuentas:</b> Participa en las oportunidades de mejora del SGSST.	<b>Incidentes:</b> Detecta y contribuye en la mejora para el control de accidentes.
<b>Peligros y riesgos:</b> Conoce la implementación que hace la empresa para prevenir cada riesgo.	<b>Artos y condiciones inseguras:</b> Notifica condiciones inseguras que se presentan en la empresa.

Ilustración 10 - App Alissta

3. Hacinamiento de los empleados: Actualmente se siguen manejando cambios de oficinas dependiendo de la cantidad de personas por proceso vs las instalaciones, para lo cual entre la Coordinación de Personal, Coordinación de Salud y Seguridad en el trabajo, Coordinación de Servicios Logísticos y la Coordinación de Infraestructura, se está realizando la verificación de

espacios para la adecuación de puntos de red, organización de puestos de trabajo y poder asignar el espacio físico adecuado para cada proceso, igualmente, esto se está realizando con apoyo de los arquitectos que están a cargo de la construcción del nuevo edificio, Positiva ARL quien además está mirando otros factores de salud ocupacional en todas las sedes asegurando consigo un adecuado espacio de trabajo para cada empleado sin que eso repercuta en la salud de las personas y generando un muy buen ambiente laboral a pesar de las cargas laborales.

Igualmente, desde Desarrollo Humano a cargo de la Coordinación de Personal, se está evaluando la posibilidad de implementar en la Institución la modalidad de teletrabajo no sólo para los docentes que imparten clases virtualmente, sino también para los trabajadores que no tengan dentro de sus actividades la atención presencial de clientes, lo cual ayudaría notablemente a la optimización de espacios. Una vez definida la cantidad de empleados que puedan trabajar de ésta forma, se debe organizar con la Coordinación de Salud y Seguridad en el trabajo las visitas a los hogares de cada empleado para verificar el que sería el puesto de trabajo por temas de enfermedades laborales, así como la asignación de una VPN, a cargo de la Coordinación de Infraestructura, la cual permitirá trabajar normalmente desde cualquier lugar, una vez verificadas y configuradas todas las reglas de conexión segura por el administrador de red de la Institución. Es importante aclarar que esto es un tema con solución a mediano plazo ya que dependiendo del personal que salga a esta modalidad, se deben verificar que las licencias de Checkpoint (VPN) estén disponibles, o de lo contrario se debe solicitar compra de más licencias las cuales no están presupuestadas y se debe solicitar dicho presupuesto a la Vicerrectoría Financiera, la cual debe entrar a mirar la viabilidad para aceptar o rechazar la compra solicitada.

Desarrollo Humano a hoy, ya ha enviado aproximadamente a 30 empleados a teletrabajo de acuerdo a las necesidades o solicitudes, y está pendiente por entregar el listado final de los empleados que salen a dicha modalidad, para ahí si poder entrar a realizar la visita y asignación de licencia.

4. Sistema de Control de Acceso: Aprovechando que el contrato de mantenimiento y soporte del sistema actualmente contratado está por vencerse, desde la Coordinación de Servicios Logísticos se empezaron a solicitar cotizaciones a diferentes proveedores, incluyendo el actual, de la implementación de las talanqueras en las sedes en las que falta y el mantenimiento de todos los equipos y de todo el sistema, que permita una operación segura teniendo en cuenta las personas autorizadas entre

estudiantes, docentes, empleados, directivos y proveedores para el ingreso a la Institución. Dicha implementación consta de una talanquera por sede con una lectora de huella y carnet que va sincronizado con el sistema de control acceso el cual permite activar o inactivar registros teniendo en cuenta retiro de personal, retiro de estudiantes, ingreso de nuevo personal y nuevos estudiantes.

Igual que el punto inmediatamente anterior, éste proceso debe pasar por la autorización de la Vicerrectoría Financiera una vez se tome la decisión del proveedor escogido para realizar la implementación del sistema de control de acceso, la cual puede llegar a tomar más tiempo teniendo en cuenta el monto requerido.

5. Comité de Seguridad de la Información: Se conformó el Comité de Seguridad de la Información, el cual está conformado por los líderes de cada proceso y el Coordinador de Datacenter que actualmente es el encargado de manejar todo lo relacionado con Seguridad de la Información, y eventualmente asiste el Rector o algún miembro del Consejo Superior.

Dicho comité, decidió realizar la contratación de un proveedor de Seguridad de la Información para que apoyen al encargado con todo el tema puesto que él no tiene el conocimiento al respecto puesto que esto hasta ahora se está empezando a trabajar en la Institución, por lo que no se tienen bases sólidas al respecto.

Con apoyo del proveedor, se estructuró el Manual de Seguridad de la Información que contiene todos lineamientos, políticas, riesgos, vulnerabilidades y amenazas de todos los activos de información de la institución, basados en la ISO 27001, para así salvaguardar la información ya sea de manera digital o física, dependiendo de la clasificación de activos realizada previamente por cada custodio, priorizándolo cada activo de acuerdo a la misión y visión de la Institución.

Éste manual de seguridad, se divulgó a todos los empleados, estudiantes y directivos de la Institución por correo electrónico y se publicó en la página web para empezar a culturizar a la gente y así cambiar el pensar, todos encaminados a un solo fin que es salvaguardar correctamente la información de la Institución tanto académica como administrativa.

Una vez divulgado el manual, se empezaron a realizar jornadas de concientización, empezando por el cambio de clave de la sesión de Windows cada determinado tiempo establecido por el comité de seguridad. Ejemplo:



*Ilustración 11 – Pieza divulgación cambio de clave*

6. Mantenimiento de equipos de red: Actualmente, se están realizando junto con los proveedores de seguridad de la información y seguridad informática, la revisión de todos los procedimientos y el mantenimiento de equipos tecnológicos y/o de software para asegurar la correcta protección de la información. En dichas revisiones se han encontrado brechas en la seguridad en el firewall, problemas de actualización del antivirus contratado, problemas en la contratación de proveedores para las cláusulas de privacidad de datos y habeas data, problemas en la correcta configuración de las VPN asignadas a ciertos empleados de la Institución.

El informe al respecto por cada proveedor se espera que sea entregado a finales de junio del 2018.

Teniendo en cuenta las actividades realizadas antes mencionadas para solucionar los problemas de seguridad que llegan a vulnerar la información de la Institución, se ve cómo muchas de las soluciones depende en gran parte del apoyo de los altos mandos de la Institución puesto que ellos son quienes toman la decisión final por el impacto que éstas generan para no afectar el normal desarrollo de actividades de la institución, lo que evidencia que un sistema de gestión de seguridad de la información, relacionado con la seguridad física, efectivamente no es sólido si no tiene el apoyo de los altos mandos para así poder promover una cultura dentro de

la Institución que permita un correcto manejo de la información dándole el lugar que ella merece, el activo más importante de la organización.



## **RESULTADOS**

Una de las actividades que se desarrolló dentro de la Institución y que generó gran impacto, fue el cambio de contraseña de inicio de sesión de Windows la cual está sincronizada con el correo electrónico. Dicho cambio se configuró mediante política del directorio activo para todos los empleados y docentes de la Institución, en donde de acuerdo a los comentarios que se escucharon dicho 12 de marzo, habían personas que nunca habían cambiado la clave desde que le entregaron su cuenta; dicha clave es una genérica la cual es de conocimiento por casi toda la comunidad institucional, lo que evidenciaba una falla en la confidencialidad y autenticación. Igualmente muchas personas manifestaban que no les parecía que se les obligara a cambiar la clave porque se les podía olvidar y podrían bloquear la cuenta, lo cual así efectivamente se evidenció, de cerca 700 cuentas entre empleados y docentes, se restablecieron 257 contraseñas, y aún hoy día, dos meses después, se siguen presentando inconvenientes de claves olvidadas. Se ha dejado claridad que dicha clave para el próximo año, estará sincronizada con los principales sistemas de información que se manejan en la institución por lo que se requiere generar la cultura de claves seguras y personales con tiempo para no tener incidentes mayores el año entrante.

El Comité seguridad de la información ha generado un impacto dividido ante la comunidad de la institución, puesto que cambiar la cultura y el pensar de la gente no es fácil, ya que sin ellos saberlo, son quienes hacen que un sistema de gestión de seguridad de la información sea exitoso, por más divulgación de políticas, de tips de seguridad y demás, si las personas no tienen la cultura, todo lo anterior no vale la pena.

En cuanto a los arreglos de Infraestructura de las sedes de la Institución, se ha visto un cambio notable en las sedes 3 y 7, puesto que se han realizado las actividades requeridas y las que salen día a día por el deterioro normal, sin embargo, se debe estar en alerta constante ante cualquier eventualidad por mínima que sea, además de realizar el mantenimiento que sea necesario de manera preventiva y no correctiva.

En cuanto a los problemas del hacinamiento de personal, la empresa de vigilancia el mantenimiento de los equipos de seguridad de redes tanto de hardware como de software, aún se está pendiente de terceros como lo son Coordinaciones de la Institución y proveedores. Éstos 3 problemas a pesar de que generan un impacto

negativo frente a la seguridad, deben seguir esperando mientras se toman las decisiones a las que hayan lugar para poder solventarlos.

## **DISCUSIÓN Y CONCLUSIONES**

- ❖ Para el salvaguardo de la información se deben tener en cuenta los riesgos de cualquier tipo que la afecten directa o indirectamente
- ❖ Minimizar los riesgos que afectan la información, toma de tiempo si no se tienen claros los activos de información más importantes de la Institución
- ❖ El apoyo de los directivos de cada compañía, en este caso de la Institución Educativa, es primordial para poder ejecutar las políticas y lineamientos establecidos dentro del sistema de gestión de seguridad
- ❖ La seguridad de la información, debe complementarse con la seguridad física de la compañía ya que ante cualquier eventualidad en cuanto a infraestructura, se debe poder asegurar la continuidad del negocio puesto que la información se mantiene intacta

## REFERENCIAS

[ Ministerio del trabajo, «Ministerio del trabajo,» [En línea]. Available:  
1 [http://www.mintrabajo.gov.co/documents/20147/36482/decreto\\_1443\\_sgsss.p](http://www.mintrabajo.gov.co/documents/20147/36482/decreto_1443_sgsss.pdf/ac41ab70-e369-9990-c6f4-1774e8d9a5fa)  
] [df/ac41ab70-e369-9990-c6f4-1774e8d9a5fa](http://www.mintrabajo.gov.co/documents/20147/36482/decreto_1443_sgsss.pdf/ac41ab70-e369-9990-c6f4-1774e8d9a5fa). [Último acceso: 26 03 2018].

[ «Iso 27000,» [En línea]. Available:  
2 [http://www.iso27000.es/download/doc\\_sgsi\\_all.pdf](http://www.iso27000.es/download/doc_sgsi_all.pdf). [Último acceso: 26 03  
] 2018].

[ D. A. C. B. Politecnico Grancolombiano, «Introducción a la seguridad de  
3 Física,» [En línea]. Available: [https://poli.epic-](https://poli.epic-sam.net/Learn/Player.aspx?enrollmentid=10870812)  
] [sam.net/Learn/Player.aspx?enrollmentid=10870812](https://poli.epic-sam.net/Learn/Player.aspx?enrollmentid=10870812). [Último acceso: 26 03  
2018].

[ Icontec, «OHSAS 18001,» [En línea]. Available:  
4 [http://www.mincit.gov.co/mintranet/loader.php?IServicio=Documentos&IFuncio](http://www.mincit.gov.co/mintranet/loader.php?IServicio=Documentos&IFuncion=verPdf&id=67471&name=NTC-OHSAS18001.pdf&prefijo=file)  
] [n=verPdf&id=67471&name=NTC-OHSAS18001.pdf&prefijo=file](http://www.mincit.gov.co/mintranet/loader.php?IServicio=Documentos&IFuncion=verPdf&id=67471&name=NTC-OHSAS18001.pdf&prefijo=file). [Último  
acceso: 26 03 2018].

[ Icontec, [En línea]. Available:  
5 [http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/fil](http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf)  
] [e/Norma.%20NTC-ISO-IEC%2027001.pdf](http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf). [Último acceso: 26 03 2018].