PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

ESCUELA DE POSGRADO

"PLAN DE COMUNICACIONES EN SEGURIDAD DE LA INFORMACIÓN PARA EL PERSONAL ADMINISTRATIVO DE LA PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ"

Tesis para optar el grado de Magíster en Comunicaciones

AUTOR

Ing. Fernando Miguel Huamán Monzón

ASESOR

Mág. Carlos José Alarco Cadillo

JURADO

Mág. Roberto Carlos Yogui Matsudo

Mág. Hugo David Aguirre Castañeda

LIMA – PERÚ

2017

INDICE

CAPÍTULO 1

1. INTRODUCCIÓN

Próxima a su centenario de vida institucional y por el inminente crecimiento de la Comunidad Universitaria, la Pontificia Universidad Católica del Perú, "comunidad de maestros, alumnos y graduados dedicada a los fines esenciales de una institución universitaria católica" (Pontificia Universidad Católica del Perú, 2014) fundada el 1 de marzo de 1917, ha puesto en marcha planes estratégicos (de larga ejecución en el tiempo) para mantener y repotenciar su prestigio como primera universidad del Perú.

Desde el año 2012 el Equipo Rectoral viene trabajando las bases (de negocio, infraestructura, servicios y tecnología) para generar el paso del modelo actual de negocio de Universidad al modelo de negocio Corporativo. En la actualidad la PUCP no sólo brinda servicios de educación superior, también otros servicios a través de sus institutos y centros de investigación.

Para su centenario de vida institucional (en el 2017) la PUCP se convertirá en un conglomerado corporativo, lo que significa, un aumento del volumen de información de lo que actualmente se administra.

En este contexto, desde el año 2011 por aprobación del Vicerrectorado Administrativo se creó el área de Seguridad de la Información con la finalidad que a largo plazo se implemente el Sistema de Gestión de Seguridad de la Información de la PUCP. En la actualidad se viene realizando el diagnóstico de las diversas unidades académicas y

administrativas para tener una visión holística del estado de madurez que tiene la Universidad en términos de seguridad de la información[1].

Uno de los factores importantes en un Sistema de Gestión son las personas. Una manera de abordar el aspecto humano es incorporar una cultura de seguridad de la información, donde la interacción de los empleados con los activos de información contribuye a la protección de estos activos. (da Veiga & Martins, 2015).

2. MARCO TEÓRICO

La información se ha convertido en un recurso clave para las organizaciones (ISACA, 2012), que se puede encontrar en distintas maneras: física, impresa, digital, etc. El concepto de seguridad ha sido trasladado también hacia la información, definiendo así la seguridad de la información como la preservación de la confidencialidad[2], integridad[3] y disponibilidad[4] de la información. (ISO - International Organization for Standardization, 2009).

¿Qué se tiene que proteger? Se ha presentado una gran gama de amenazas a la información. Teniendo en claro la amenaza como "todas las actividades, eventos o circunstancias que pueden afectar el buen uso de un activo de información dañándolo y no permitiendo que brinde soporte a algún proceso, perjudicando directamente la consecución de los objetivos de negocio" (Tupia, 2010).

Tupia (2010) pone en diagrama la relación entre la amenaza, la información y cómo afecta a una organización.

[1] Fuente: Reporte de Gestión de la Oficina de Contraloría 2014 (*reporte confidencial*)
[2] **Confidencialidad**: Restringir el acceso y la revelación de la información a las personas correctas.
[3] **Integridad**: Proteger contra una modificación o destrucción impropia de información.
[4] **Disponibilidad**: Asegurar un acceso y un uso a tiempo y fiable de la información.

Figura 1 - Esquema Amenaza-Activo-Riesgo-Impacto

Las amenazas son los eventos supuestos que pueden afectar a la información. De materializarse, se convierte en riesgo y tiene un impacto a la organización.

Para evitar que estas amenazas se materialicen, las organizaciones comienzan a diseñar e implementar ciertos controles que permitan reducir la probabilidad e impacto que se materialicen estas amenazas. Según lo definido por COBIT 5 (2012) los controles son los medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras organizativas, que pueden tener una naturaleza administrativa, técnica, de gestión, o legal.

Una encuesta realizada a nivel mundial en el 2014 por PwC - PricewaterhouseCoopers evidenció que del total de incidentes de seguridad de la información, un 58% fue **por consecuencia de empleados y ex empleados** (PricewaterhouseCoopers, 2014). Curiosamente, los resultados de la encuesta indican que el número de **incidentes reales imputables a los empleados ha aumentado** en un 25% desde la encuesta de 2013.

Adicionalmente, las investigaciones realizadas por el Instituto Ponemon indicaron que las infracciones **se debieron a factores humanos (35%)**, problemas del sistema (29%) y los ataques maliciosos o criminales (37%). (Ponemon Institute, 2013)

Si nos basamos en estos dos estudios anteriores, los colaboradores actuales (y también ex colaboradores) son considerados como una de las causas fundamentales de los incidentes

de seguridad de la información. Una manera de abordar el aspecto humano es incorporar una **cultura de seguridad de la información**.

Según The BMIS (ISACA, The Business Model for Information Security, 2010), la Cultura se define como "un patrón de comportamientos, creencias, suposiciones, actitudes y formas de hacer las cosas". ISACA en su publicación Creating a Culture of Security resalta que "todas las empresas tienen una cultura en seguridad de la información. En la mayoría de los casos carece de intencionalidad y es inconsistente a las medidas que existen; en otros, es robusta y guía las actividades diarias de los empleados y otras personas que entran en contacto con la empresa" (ISACA, Creating a Culture of Security, 2011)

El Marco de Negocio para el Gobierno y Gestión de las Tecnologías de Información COBIT 5, define el Ciclo de Vida de la Cultura de Seguridad de la Información como un factor que trasciende a toda la organización (ISACA, 2012). La cultura es influida por factores externos e internos (como el estado, la competencia, los proveedores, los clientes, los trabajadores, grupos de interés, entre otros) y se constituye por el comportamiento (organizacional e individual) y el nivel conciencia en seguridad de la información (que puede aumentar o disminuir). (ISACA, 2012)

El **ANEXO I** detalla los ocho comportamientos ideales (definidos por ISACA en COBIT 5 for Information Security) que debería tener una organización (se debe considerar en dos niveles: nivel organizativo y nivel individual). En lo individual que concierne en el ámbito de las personas, se destaca que:

- A las personas les importa el bienestar de la organización y en consecuencia aplican las técnicas en seguridad de la información.

- Las personas han leído, comprendido y se sienten capacitados con las políticas y principios de seguridad de la información.
- Las personas se animan a participar y cuestionar la situación actual de la seguridad de la información.
- Las personas comprenden su responsabilidad con la seguridad de la información.
- Las personas saben reconocer un incidente de seguridad de la información y cómo debe de notificar y reaccionar.
- Las personas aportan nuevas ideas para la seguridad de la información.

La cultura de seguridad de la información (que incorpora una interacción de los empleados con los activos de información) contribuye a la protección de estos activos. En otras palabras, es fundamental esta interacción para mejorar la cultura de seguridad de la información en las organizaciones, lo que traerá como consecuencia el buen comportamiento de los empleados en el cumplimiento de seguridad de la información y las políticas de procesamiento de información relacionada y los requisitos reglamentarios. Esto se puede lograr mediante la evaluación, seguimiento de cómo los empleados cumplen con las políticas de seguridad de la información y así influir en la cultura de seguridad de la información.

Estos ocho comportamientos ideales serán tomados como referencia para la medición del Plan de Comunicación de Seguridad de la Información según el alcance del proyecto. Si bien son 8 los comportamientos, éstos pueden disgregarse en una cantidad mayor que permita tener más a detalle las características del comportamiento que debe tener un grupo de personas (que tengan características en común).

Es importante entender la cultura existente, para generar cambios positivos que permitan alcanzar una cultura de seguridad de la información adecuada. Estos cambios se llevan a

cabo mediante el uso de herramientas, descritas como buenas prácticas. (ISACA, 2012). En ese sentido, el diagnóstico a ejecutarse contemplará el conocimiento de la cultura actual de la seguridad de la información.

Las herramientas para crear, fomentar y mantener una cultura deseada en seguridad de la información en toda la organización incluyen:

Buenas Prácticas		
Comunicación	**Líderes**	**Incentivos y Recompensas**
• Estrategias para comunicar a toda la organización los comportamientos deseados y los valores organizacionales en seguridad de la información.	• Esta difusión de los comportamientos deseados será reforzada con el comportamiento ejemplar de la Alta Dirección y/o otros líderes de la organización.	• Los incentivos para alentar y medidas disuasorias para hacer cumplir las actitudes, normas y reglas que proporcionan una mayor orientación sobre los comportamientos deseados y relacionan muy claramente con los principios y políticas de seguridad de la información de la organización

Figura 2 - Buenas Prácticas para la Cultura en Seguridad de la Información

Estas tres herramientas serán consideradas en el diseño e implementación del programa de concientización. Es preciso indicar que, sobre todo, la práctica "Incentivos y Recompensas" puede demandar un gasto y presupuesto adicional por parte de la Universidad (a través de su área de Seguridad de la Información). Si se tomase esta buena práctica como estrategia final del presente proyecto, deberá ser evaluado respecto al presupuesto a asignarse a dicha actividad.

En la investigación realizada para el presente proyecto se encontraron términos relacionados a la creación de cultura: concientización, entrenamiento y educación. Es preciso poder aclarar términos y reconocer las relaciones que tienen todos enfocados a seguridad de la información.

La concientización busca llegar a las personas mediante técnicas y formas atractivas para que centren su atención en la seguridad de la información generando la capacidad de reconocer los riesgos de seguridad de TI y así puedan actuar de manera consecuente sobre la administración de la información que está a su cargo. (NIST, 2015)

El entrenamiento busca enseñar habilidades que permitan a una persona realizar una función específica. Las habilidades adquiridas durante el entrenamiento se construyen sobre la base de la concientización (mediante contenidos de conceptos, teorías y buenas prácticas de seguridad de la información) (NIST, 2015)

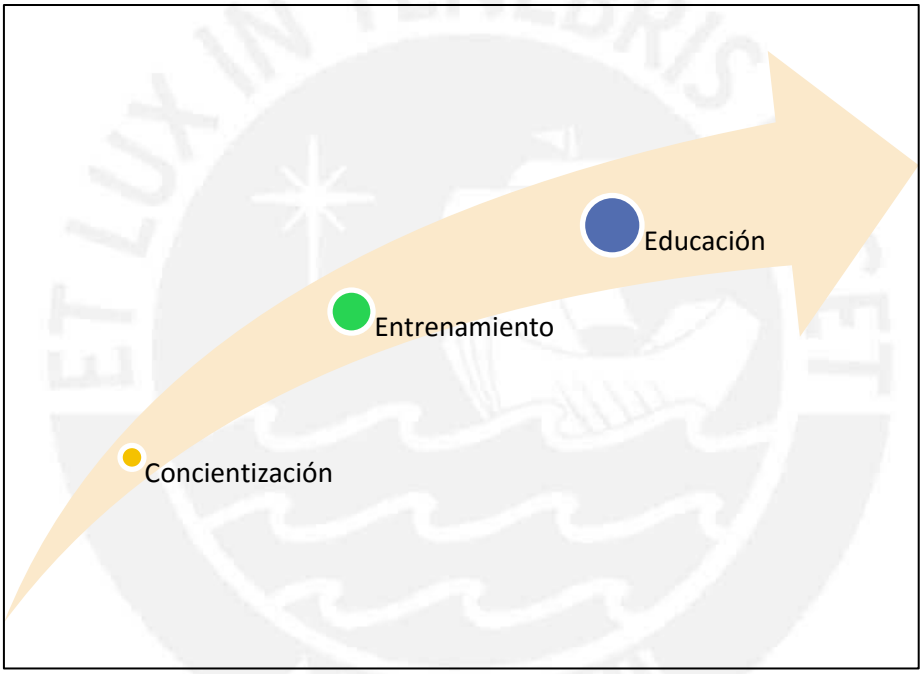


Figura 3 - Educación en Seguridad de la Información (elaboración propia tomando como referencia NIST 108)

La educación es el punto de evolución que proviene de la formación y es el resultado de la acumulación de actividades que impulsen la conciencia de las personas en temas de seguridad de la información. (Herold, 2005)

La ENISA - European Union Agency for Network and Information Security en base a lo determinado por Wilson y Hash propone tres procesos principales en el desarrollo de un programa de Concientización de Seguridad de la Información:

Figura 4 - Procesos principales en el desarrollo de un Programa de Concientización

A continuación se desarrolla cada proceso:

Proceso	Descripción
1. Planificar, Valorar y Diseñar	El Programa de Concientización debe estar Alineado a la misión de la organización y apoyar a sus necesidades. Debe ser un factor importante de la cultura de la organización y de su Arquitectura de TI. Los Programas más exitosos son los que generan que el usuario se sienta un factor importante en la estructura de seguridad de información de la organización. En la etapa de diseño del Programa se identifican las necesidades para crear conciencia en seguridad de la información, se desarrolla un plan eficaz de concientización, se solicita que sea aprobada por la entidad más alta de gobierno de la organización y se fijan prioridades.
2. Ejecutar y gestionar	Todas las actividades para implementar un programa de concientización sobre seguridad de la información. Sólo se puede iniciar cuando: 1. Se ha evaluado las necesidades. 2. Se ha desarrollado una estrategia. 3. Se ha diseñado un plan de programa de concientización. 4. Se ha desarrollado contenidos de concientización.

3. Evaluar y mejorar	Son componentes críticos de cualquier programa de concientización. Se requiere saber cómo está funcionando el programa existente para generar mejora continua. Además, el proceso de retroalimentación debe ser diseñado para enriquecer los objetivos iniciales del programa. Se debe definir una línea base para diseñar e implementar una estrategia de retroalimentación.

Tabla 1 - Procesos principales en el desarrollo de un Programa de Concientización

Para la base teórica Comunicacional, el proyecto tendrá como punto de partida el modelo de comunicación de Shannon y Weaver: Teoría de la Información (Shannon & Weaver, 1981), por integrar todos los elementos que se pueden identificar para el desarrollo de este proyecto: fuentes, emisor, canal, receptor, destinatario, ruido.

Anecdóticamente, este modelo de comunicación fue la base para el desarrollo de la informática, ciencia que enmarca a la seguridad de la información y que es el punto central de este proyecto de comunicación.

Al tratarse de un escenario de cambio de conducta, es necesario resaltar que se involucran múltiples factores internos (conocimientos, creencias, entre otros) y factores externos (interacciones sociales, entorno en el que se desenvuelven).

Desde la psicología existe el Modelo Transteórico y la Teoría Social Cognitiva entre las más usadas. El modelo transteórico de Prochaska y DiClemente es también conocido como el Modelo de Etapas de Cambio consiste en aplicar, según la etapa de cambio en la que se encuentre la persona, intervenciones personalizadas (Prochaska & Diclemente, 1983). Estas etapas de cambio son la precontemplación, contemplación, determinación, acción, mantenimiento y recaída. La Teoría Social Cognitiva consiste en la observación de las personas e identificar su conducta teniendo como elemento básico el nivel de confianza que tiene la persona en realizar una actividad concreta (con un objetivo concreto)se basa en la importancia de observar a las demás personas y aprender de éstas,

así como en el refuerzo positivo y negativo de la conducta (Bandura, 1977).

En el 2011, un grupo de investigadores propusieron el modelo de "The behaviour change Wheel" (Michie, 2011) que, para efectos del presente proyecto, permitirá diseñar las intervenciones comunicacionales para lograr los cambios de comportamientos que se fijen. Si bien este modelo ha sido usado para el campo de la salud, se propone la respectiva extrapolación al ámbito de seguridad de la información.

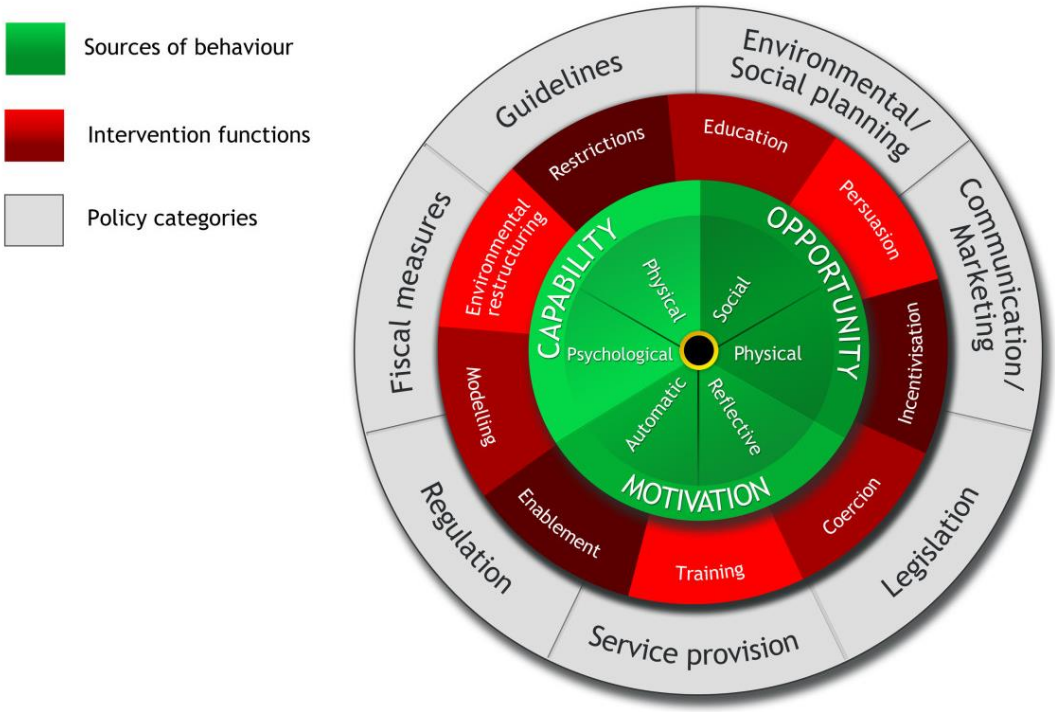


Figura 5 - "The behaviour change Wheel" (Michie, 2011)

El modelo contiene 3 ruedas, la primera (de color verde) presentan las condiciones en una persona para el cambio: Las capacidades (es decir, los conocimientos y habilidades de la persona), la motivación y la oportunidad (los factores externos que juegan un papel de habilitadores para el cambio). La segunda rueda (de color rojo) se presentan la diversidad de intervenciones para realizar el cambio de comportamiento: la formación, las restricciones, la persuasión, los incentivos, la reestructuración del entorno, la educación, las medidas coercitivas, la capacitación y la modelización. Y por último (color plomo) se

presenta las directrices o políticas que brindan el contexto para realizar las intervenciones para el cambio de conducta (como son: las directrices, la planificación del contexto, la comunicación, la legislación, la prestación de servicios, la regulación y la fiscalización)

Este modelo permitirá diseñar de manera más óptima las actividades comunicacionales que brindarán la base para el cambio de cultura (de comportamiento) en los colaboradores administrativos de la PUCP respecto a la seguridad de la información que administran y está bajo su custodia.

3. MARCO REGULATORIO

Desde mayo de 2013 se encuentra vigente en el Perú la Ley 29733 – Ley de Protección de Datos Personales que es afecta a todas las organizaciones públicas y privadas que ejercen sus funciones, ofrecen productos y servicios en el mercado peruano.

Ante esto, la PUCP es afecta a esta legislación en la que se podría verse, en caso de no-cumplimiento, inmersa en multas que se encuentran en un rango de 1UIT[5] a 100UIT.

El cumplimiento de esta Ley implica no sólo medidas técnicas de seguridad y legales, sino que incluyen medidas organizativas, las cuales están directamente involucradas con el comportamiento de las personas (colaboradores) respecto a la información que administran.

En el mismo sentido, la PUCP cuenta con convenios de servicios de empresas, los cuales son celebrados con pre-requisitos de seguridad de la información. Ejemplo de ello es el

[5] **UIT**: Unidad Impositiva Tributaria. En el Perú una UIT tiene el valor de S/. 3,950.00

cumplimiento de alineación de los procesos (es decir, el involucramiento de las personas) a la norma internacional PCI-DSS para el uso de tarjetas de crédito.

El no-cumplimiento de este requisito podría ocasionar el término de estos convenios.

4. DEFINICIÓN DE LA PROBLEMÁTICA

La problemática identificada inicialmente se enmarca en toda la Comunidad Universitaria de la PUCP (es decir: docentes, administrativos y alumnos) y respecto al nivel de cultura de seguridad de la información con la cuenta este grupo de personas.

Sin embargo, es prioritario destacar la diferencia de perfiles entre estos 3 subgrupos dentro de la Comunidad Universitaria. Para ello, se tendrá que analizar la pertinencia del alcance del presente proyecto, sobre todo en la determinación del público primario.

Las buenas prácticas han de ser insertadas en la cultura organizacional (Tuck School of Business at Dartmouth, 2011), según recomienda un informe realizado por la Tuck School of Business. Las buenas prácticas han de estar inmersas en el día a día laboral de los colaboradores de la organización.

5. DIAGNÓSTICO

En base a la encuesta realizada al personal docente y administrativo (ver **ANEXO II**) se estructuró la información levantada en tres grupos: 1) los conceptos y terminología de Seguridad de la información; 2) Incidentes de Seguridad; y 3) Personas: Comportamiento, hábitos y buenas prácticas.

Conceptos y terminología de Seguridad de la Información

Los encuestados, en general, asocian la Seguridad de Información con el cuidado y resguardo de toda información tanto en dispositivos electrónicos como de documentos en físico. Algunas personas, no obstante, sólo consideran que la Seguridad de Información refiere a la información digital o todo aquello relacionado a tecnología.

Un dato relevante en las respuestas analizadas es que para muchos usuarios la responsabilidad recae en las medidas que toma la Universidad respecto al tema, tales como la generación de políticas e incluso del respaldo de la información; más que en su propia responsabilidad.

Dentro de los ejemplos de medidas de Seguridad de la Información, se recopiló lo siguiente:

- Cambiar periódicamente la contraseña de las cuentas de correo electrónico.
- Usar correctamente de los dispositivos electrónicos para menguar el ingreso de virus informáticos.
- Cuidar los documentos en físico mediante compartimientos con llave.
- Al momento de botar a la basura o al reciclar documentos que contengan información confidencial, estos deben ser destruidos acuciosamente.
- Evitar la exposición de información (virtual, documentos en físico, información verbal) a terceros que puedan interpretar o emplear la información de forma errónea.
- Conocer las medidas preventivas como Seguridad de la Información.
- Conocer las alternativas de reacción frente a incidentes en Seguridad de la Información.

Si bien las ideas expresadas son acertadas (según la terminología usada por la ISO27001[6]), en muchos casos solo consideran un aspecto u otro; por lo cual, es necesario diseñar una campaña que explique toda la información concerniente a Seguridad de la Información; y, sobre todo la responsabilidad de cada usuario.

Al preguntar sobre el concepto de virus informático que manejan los administrativos y profesores se pudo relevar que los encuestados consideran a los virus informáticos:

- Dañinos.
- Riesgosos, por lo cual es necesario tomar precauciones.
- No atacan únicamente a personas que entrar a páginas no deseadas.

La alternativa que causó mayor controversia, en ambas muestras, es la de aceptar que son nocivos pero que solo se previene con el correcto uso de internet. En el área administrativa, el 46% está de acuerdo con esta afirmación, mientras que el 42% rechaza el enunciado. Por otro lado, el área académica se muestra renuente al postulado en un 51%, 36% está a favor y el 13% dejó de contestar.

Aproximadamente un tercio de la muestra total sí considera que tienen un rol dentro de la Seguridad de la Información, en muchos de estos casos, comparten la responsabilidad con distintas entidades de la Universidad.

[6] **ISO27001**: Estándar ISO sobre Seguridad de la Información.

Se puede concluir que muchos usuarios no se consideran responsables de la Seguridad de la Información, delegando esta labor a otras entidades. Profesores y administrativos identifican a DTI como el principal responsable de los temas relacionados a Seguridad de la Información.

Ante la pregunta, ¿Tiene la Universidad una unidad o persona asignada para labores exclusivas de Seguridad de la Información?, se puede observar una diferencia entre la perspectiva del área administrativa y el área académica, ya que más de la mitad del área administrativa (51%) comentan que no hay una unidad o persona encargada en los temas de Seguridad de la Información; mientras que más de la mitad del área académica (58%) comenta que sí hay un personal a cargo de ello.

Los colaboradores que sí reconocen la existencia de un área, afirman que las unidades encargadas de ver temas de Seguridad de Información son Contraloría, DTI[7] y Seguridad Informática.

Incidentes de Seguridad

Al realizar la pregunta: ¿Qué entiende por incidente en Seguridad de la Información?, las respuestas expuestas giran en torno a las siguientes afirmaciones:

- Pérdida de información que no está resguardada y es irrecuperable.
- Acceso de personal externo a información de la PUCP.
- Intento de ingreso a información personal electrónica del usuario.

[7] **DTI**: Dirección de Tecnologías de Información de la Universidad.

- Cualquier filtro de información confidencial (incluso información compartida de manera verbal).
- Ingreso de un virus a la computadora.
- Ingreso al correo del usuario por parte de un tercero.
- Hackeo de la computadora laboral o personal (en el caso del área académica).

El área administrativa reconoció, en su mayoría, como incidente de Seguridad de la Información el filtro de información confidencial que puede tener mal uso. Por otro lado, el área académica asoció con mayor frecuencia, como incidente en Seguridad de la Información, la presencia de algún virus informático en sus computadoras.

Asimismo, ambas áreas coinciden en calificar la pérdida de información como un incidente severo que puede tener consecuencias graves.

De esta manera, se debe difundir en los usuarios los distintos tipos de incidentes en Seguridad de la Información y brindar alternativas de prevención que puedan auto gestionar como la realización de copias de respaldo.

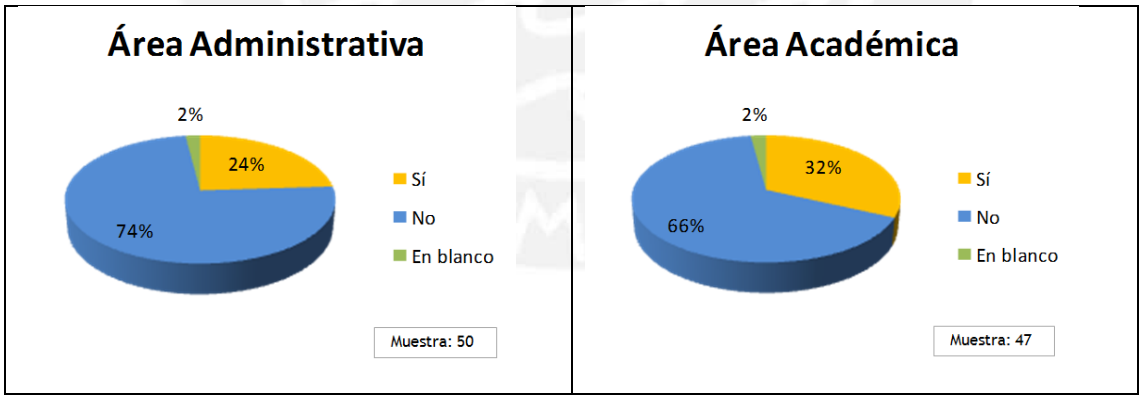


Figura 6 - ¿Ha sido vulnerable por un incidente de seguridad?

Se presenta que la población del área académica es más vulnerable a incidentes en Seguridad de la Información en un 32%, a diferencia del área académica que presentan 24% de probabilidad.

Al pedir que especifiquen cuáles han sido los incidentes más comunes, las razones manifestadas en ambas áreas son similares e indican lo siguiente:

- Presencia de virus informáticos en sus computadoras.
- Problemas con el servidor interno de la PUCP.
- Correos de destinatarios desconocidos solicitando información del usuario (incluso haciéndose pasar por la PUCP).
- Problemas con los USB.

Personas: Comportamiento, hábitos y buenas prácticas.

Ante la pregunta ¿Con qué frecuencia realiza copias de respaldo de su información? Se identificó que más de la mitad de ambas áreas nunca o casi nunca realizan copias de información. En el caso del área administrativa, el 32% no realizan copias de la información y el 22% lo realiza de manera muy eventual (dos o tres veces al año). En el caso del área académica, el 21% no realiza copias de respaldo y el 36% lo realiza de manera muy eventual (dos o tres veces al año).

Al consultar sobre los dispositivos donde los usuarios visualizan su cuenta de correo electrónico, tanto en el área administrativa como el área académica (ver **Figura 4**), más de la mitad de colaboradores hacen uso de una computadora para visualizar el correo electrónico; encontrándose un mayor uso de la computadora de trabajo en el personal administrativo (43%).

Mientras que, en el caso del personal académico, presentan igual frecuencia en la computadora personal y del trabajo. Además, se observa muy poco uso de otros dispositivos como Tablet o Smartphone.

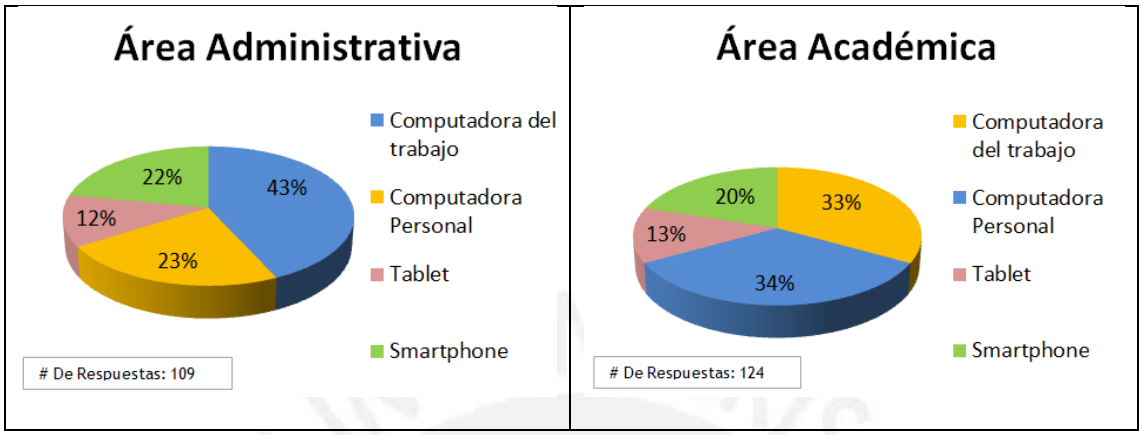


Figura 7 - Dispositivos desde donde visualizan cuentas de correo

Tanto en el área administrativa como académica, no se han recibido capacitaciones o inducciones de Seguridad de Información. No obstante, en caso se haya presentado alguna capacitación, se observa más en el personal administrativo. (Ver **Figura 8**)

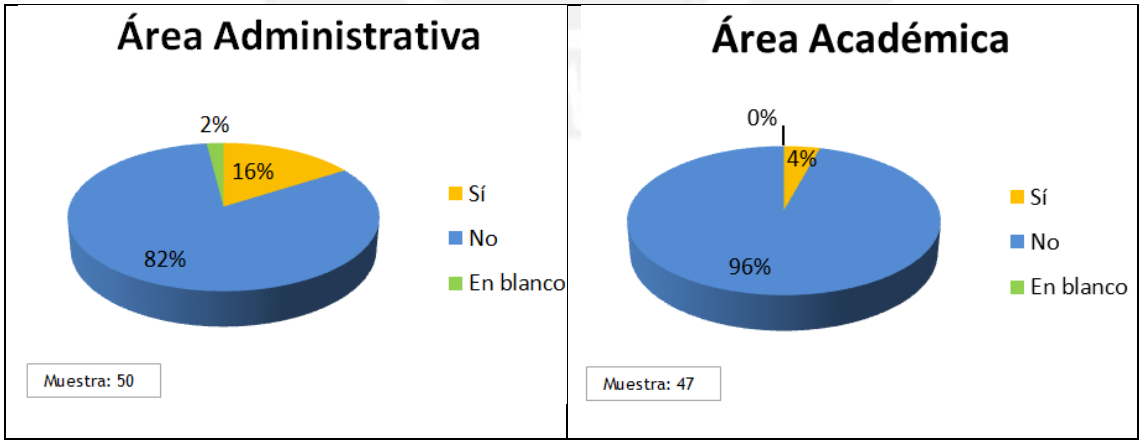


Figura 8 - Capacitaciones en Seguridad de la Información

5.1. CONCLUSIONES PRELIMINARES

En base a lo relevado por medio de la encuesta al personal administrativo y docente, se estructura a manera de conclusiones previas de la problemática en la Universidad, lo siguiente:

1. Se identificó que la población encuestada cuenta con información parcial sobre Seguridad de la Información. Aunque cuentan con ideas básicas del tema, no consideran todo lo que Seguridad de la Información implica.

2. Se identificó que uno de cada tres usuarios ha experimentado algún incidente en Seguridad de la Información. Estos se presentan en mayor magnitud en el personal académico que en el personal administrativo. Asimismo, se encontró que entre los incidentes más comunes están: la presencia de virus informáticos, problemas con los USB, recepción de correos solicitando información personal del usuario o inclusive contraseñas, entre otros.

   Es importante mencionar que la mayoría de la población es vulnerable a estos incidentes; es por ello, deben contar con información completa que les permita tomar las medidas adecuadas para afrontar una situación de este tipo.

3. Se evidenció la falta de información del usuario con respecto a Seguridad de la Información, pues se encontró que el 50% de la población asevera que el encargado es la DTI. Este resultado evidencia la falta de conocimiento básico del usuario, que requiere ser difundido.

4. Se identificó que los usuarios no asumen la responsabilidad esperada en los temas de Seguridad de la Información, pues buscan encargados externos. Uno de los principales objetivos del proyecto de Concientización en Seguridad de la Información es que el usuario tome conciencia del rol que cumple e interiorice medidas de prevención.

5. El 73% de la población es consciente de la necesidad de hacer copias de seguridad de su información; sin embargo, solo el 44% del total llevan a cabo este hábito en un periodo menor de un mes. El 29% restante maneja otra frecuencia que puede ser entre los dos (2) a seis (6) meses; incluso, anualmente. Además, el 27% de usuarios no realiza copias de respaldo alguna de su información, siendo vulnerables a un incidente donde pueda darse la pérdida de información laboral y personal.

5.2. GESTIÓN DE INFLUENCIA

De acuerdo a las entrevistas realizadas al Contralor General de la PUCP y al Oficial de Seguridad de la Información de la PUCP (ver **ANEXO VI**), se obtuvieron los siguientes resultados sobre el potencial de influencia y la gestión de la influencia del área de seguridad de la información.

5.2.1. Potencial de la Influencia del área de Seguridad de la Información

Notoriedad:

En consecuencia, de las propias funciones de la Oficina de Contraloría (unidad a la que pertenece actualmente el área de seguridad de la información) se ha logrado un

conocimiento del área. Sin embargo, al ser la Oficina de Contraloría un ente de control y auditoría, se percibe al área de Seguridad de la Información como parte del control posterior a las acciones que tengan en las unidades.

El rol de la seguridad de la información debe de ser inmersa en las funciones de cada unidad, como parte de su día a día.

Representatividad:

Sólo en una unidad administrativa tiene insertado en sus funciones un nivel intermedio de seguridad de la información. La representatividad es para todo el eje administrativo (13 unidades administrativas)

Compromiso:

Los principales ejecutores de la influencia son los jefes y directores de las unidades administrativas. Sobre su nivel de compromiso, sólo se tienen a 2 directores concientizados en seguridad de la información de un total de 13.

Es un punto importante llegar a crear conciencia a los 11 jefes de unidades restantes.

Notabilidad:

La función de seguridad de la información es considerada dentro de la organización como un “apaga incendios”. Es decir, se percibe a los esfuerzos de seguridad de la información como controles reactivos en consecuencia de algún incidente que haya afectado a la confidencialidad de la información.

En este punto es necesaria la intervención comunicacional para cambiar la percepción del personal administrativo para que se tenga a la función de seguridad como recomiendan las buenas prácticas internacionales: como un rol preventivo.

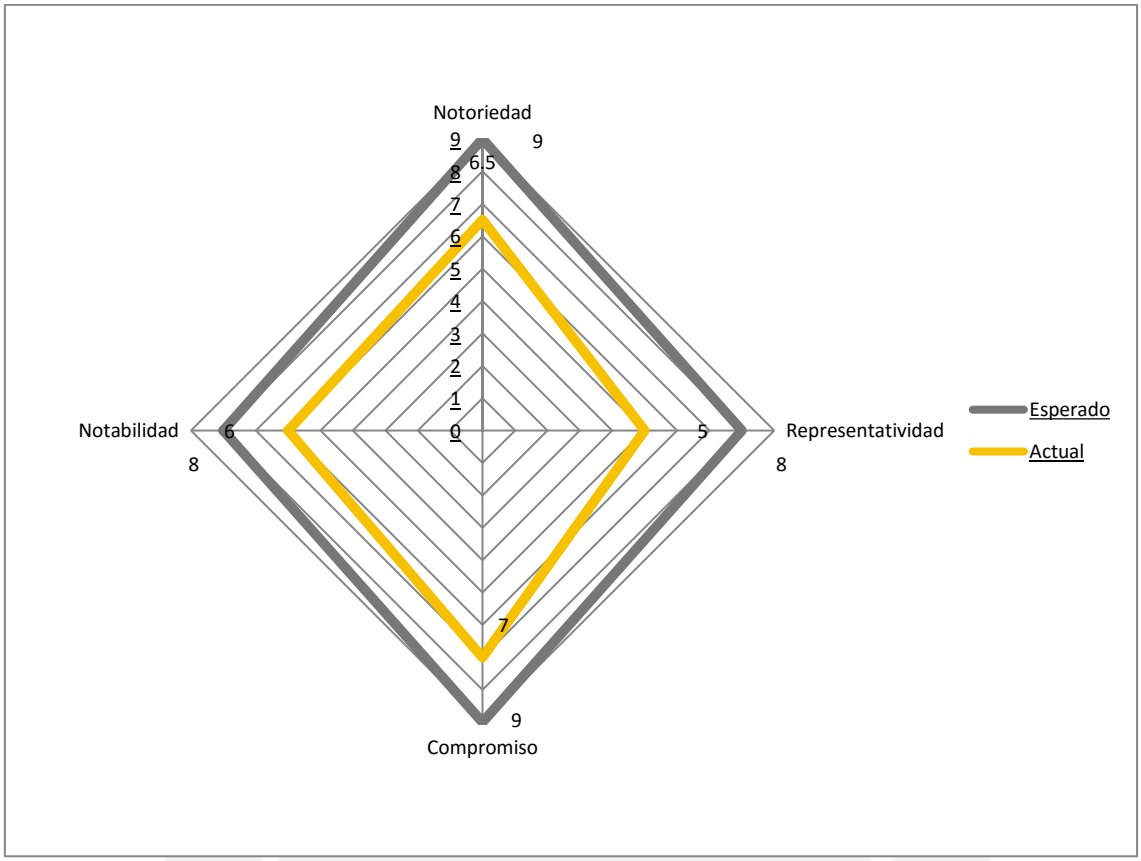


Figura 9 - Potencial de Influencias

5.2.2. Gestión de la Influencia

Estratégico:

La Oficina de Contraloría reporta directamente al Equipo Rectoral de la Universidad, lo que posiciona estratégicamente al área de Seguridad de la Información para el desarrollo de los planes que se diseñen. Es importante recalcar que el área de Seguridad de la Información tiene mayor influencia en las unidades adscritas al Vicerrectorado Administrativo.

Sistemático:

Las vías y plataformas de comunicación se encuentran en un proceso de maduración de sistematización. La Dirección de Comunicación Institucional dispone las directrices de las comunicaciones internas de la Universidad mediante protocolos y procedimientos para estos fines. Se apoya mucho en las herramientas tecnológicas tanto para el diseño como el monitoreo de las acciones de comunicación ejecutadas.

Proactivo:

En la actualidad los esfuerzos de seguridad de la información se refieren sólo como reacción a un incidente que pueda haberse presentado (al igual que las comunicaciones). Se requiere impulsar la elaboración de procedimientos y/o protocolos que permitan tener un perfil más proactivo y de prevención, antes de sólo reacción.

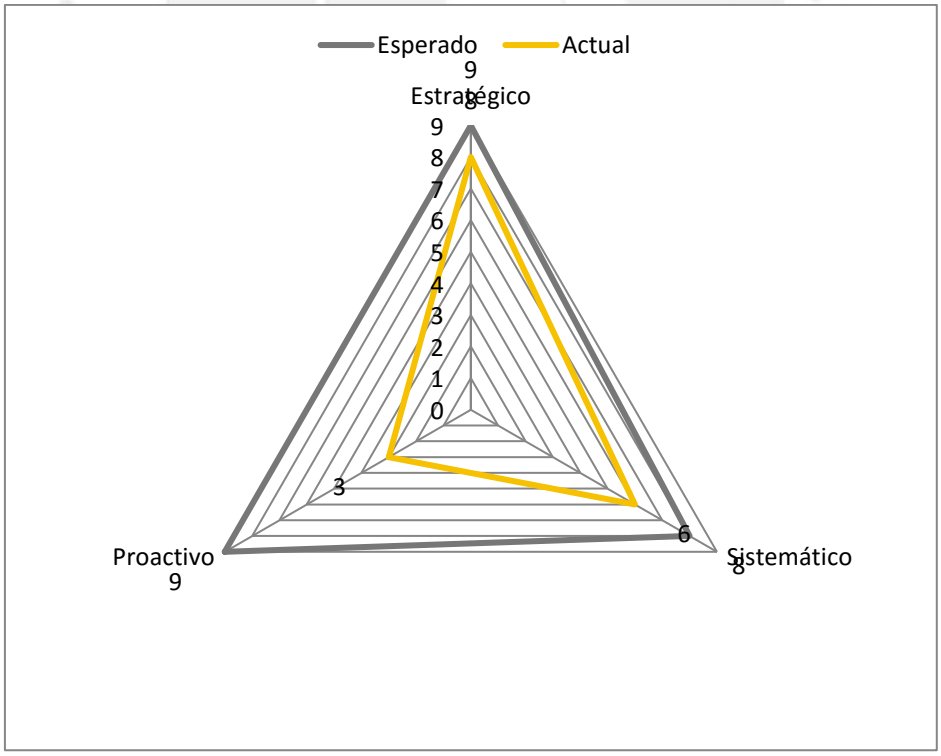


Figura 10 - Gestión de la Influencia

5.3. PÚBLICOS

La Pontificia Universidad Católica del Perú está conformada por la Comunidad Universitaria (alumnos, profesores y administrativos). En términos numéricos la Comunidad Universitaria está distribuida de la siguiente manera:

Comunidad Universitaria	Cantidad
Estudiantes (pregrado y posgrado)	26,866
Profesores	2,825
Administrativos	2,925

Tabla 2 - Cifras de la PUCP[8]

Las relaciones entre estudiantes, profesores y administrativos (ver **Figura 11**) responde a la estructura funcional que tiene la Universidad. El estudiante es el cliente final (y el más importante) de la Universidad, el cuál (en su mayoría) consume el servicio de educación mediante un curso. El profesor, que pertenece a un Departamento Académico, es designado por este último para dictar cursos según requerimientos de una Facultad. El personal administrativo brinda un soporte a las actividades y funciones tanto de los Departamentos Académicos (profesores) y de las Facultades (alumnos y profesores).

[8] http://www.pucp.edu.pe/la-universidad/nuestra-universidad/pucp-en-cifras/

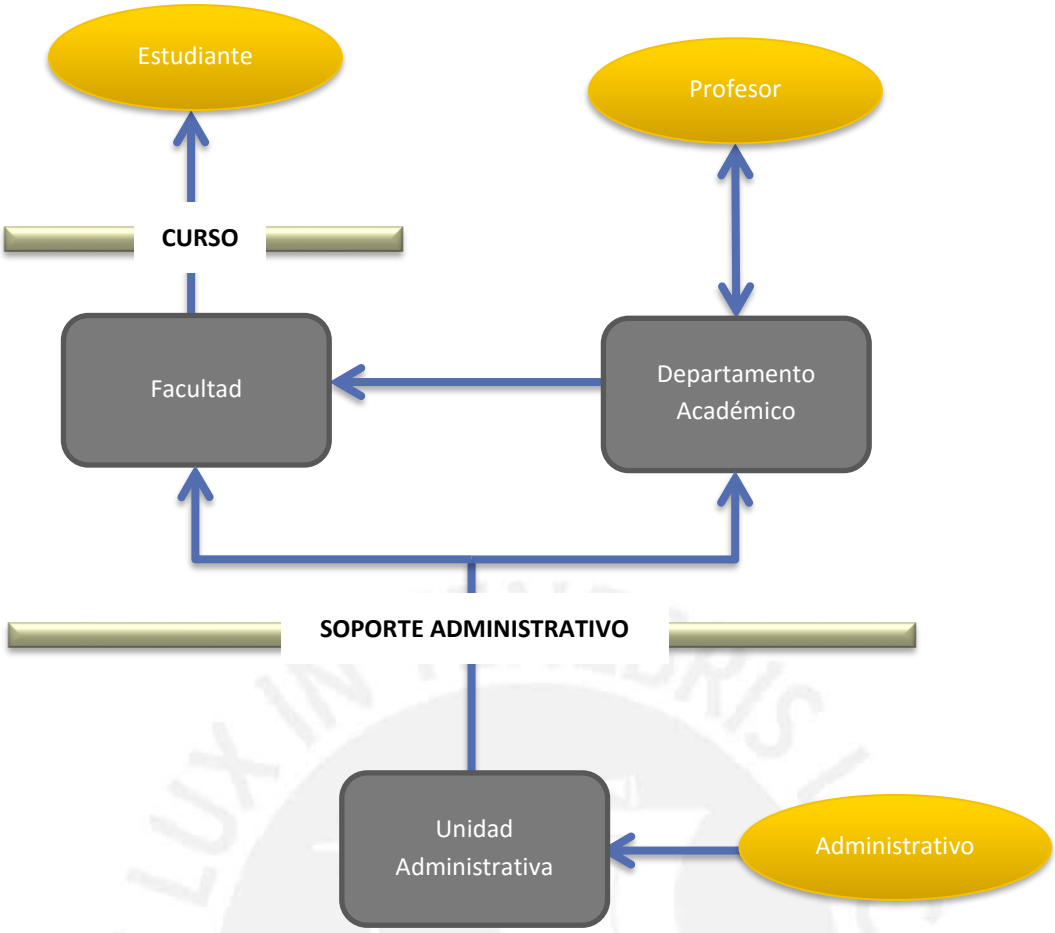


Figura 11 - Relaciones entre estudiantes, profesores y administrativos

Sin embargo, a efectos de la aplicación del presente proyecto, considerando tiempos de ejecución y alcance de presupuesto, sólo se atenderá al público administrativo. Se deberá considerar si se atiende al personal administrativo en iniciarlo en la cultura de seguridad de la información, ya que esto permitirá estructurar una base sólida en la Comunidad Universitaria, debido a que son los que brindan el soporte al cliente interno (profesores) y al cliente externo (estudiantes).

5.4. POLÍTICAS Y PROGRAMAS EXISTENTES

En la actualidad, en la Universidad, existen ciertas políticas y programas que están relacionadas con el presente proyecto:

Política de Seguridad de la Información

Mediante la revisión del marco documentario relacionado a seguridad de la información existente en la PUCP, se evidenció la elaboración de una Política General de Seguridad de la Información que presenta once (11) artículos de carácter técnico-especializado sobre la directriz de seguridad de la información que tiene como intención la Universidad.

Este documento, sin aprobación por las altas autoridades de la Universidad, además de ser muy extenso (58 páginas) ha sido elaborado en términos especializado de seguridad de la información.

A efectos del diseño de la estrategia tendrá que ser tomado como referencia y punto de partida, más aún deberá de traducir los mensajes a términos que puedan ser socializados a los diferentes tipos de públicos que atenderá el presente proyecto.

Sesiones de Inducción en Seguridad de la Información

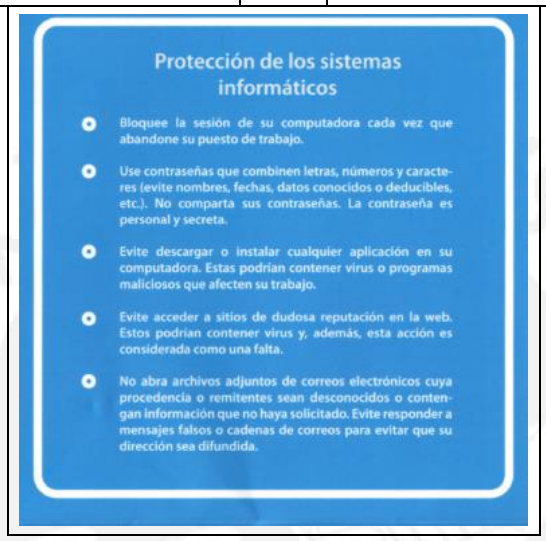
Quincenalmente el área de Recursos Humanos de la Universidad realiza programas de inducción institucionales al personal nuevo (que desempañará alguna tarea administrativa) en las que además de información de la universidad, planillas, beneficios, se les presenta a los nuevos colaboradores de la universidad los programas de interés para la Universidad: seguridad y salud en el trabajo, responsabilidad social, seguridad de la información, entre otros.

Figura 12 - Sesión de Inducción de Seguridad de la Información

El área de seguridad de la información tiene a su disposición una sesión de 20 minutos de duración para difundir sus buenas prácticas en el resguardo de la información de la Universidad a sus colaboradores.

Para esto, el área de seguridad de información de la PUCP ha diseñado un decálogo de seguridad de la información y merchandising de seguridad de la información que es repartido a los colaboradores de la Universidad.

Este decálogo contiene 10 tips de seguridad de la información sobre documentos impresos, la confidencialidad de la información y la protección de los sistemas informáticos.



El merchandising consiste en mouse-pads y lapiceros con el logo del área de seguridad de la información. Además cuentan con blocs de notas que contienen tips de seguridad de la información como pie de página en cada hoja.

Si bien existen estos 3 elementos de difusión, no están articulados ni responden a una estrategia formalizada, integrada, ni coordinada de comunicación. Será motivo de análisis el diseño de una estrategia en la que se incluya estos elementos y/o proponer mejoras a los mismos.

5.5. CAPACIDAD DE LA INSTITUCIÓN

A efectos del presente proyecto y considerando los factores requeridos para atender el problema planteado, la Universidad cuenta con la siguiente capacidad institucional:

Área de Seguridad de la Información:

Se encarga de atender las necesidades de las unidades en resguardar la confidencialidad, integridad y disponibilidad de su información. Tiene como función asegurar la confidencialidad, integridad, exactitud y oportunidad del procesamiento de la información, procurando y controlando el cumplimiento de las políticas, normas y procedimientos de seguridad de la información.

Dirección de Comunicación Institucional:

La Dirección de Comunicación Institucional (DCI) es la unidad responsable de la planificación estratégica y definición de las políticas de comunicación de la Universidad. Gestiona y regula la comunicación de las direcciones académicas y administrativas, facultades, departamentos y centros e institutos.

Mediante su área de Comunicación Interna, gestiona las necesidades de comunicación de las unidades institucionales desarrollando estrategias que aporten al cumplimiento de sus objetivos además de capacitar a quienes gestionan la comunicación en las unidades con la finalidad de fortalecer el vínculo entre la comunidad universitaria y la institución.

Dirección de Recursos Humanos:

La Dirección de Recursos Humanos tiene como función gestionar y facilitar el desarrollo de los colaboradores administrativos.

Su sección de Capacitación tiene como función brindar entrenamiento a todo el personal de la Universidad en temas que respondan a necesidades reales de la institución. Para ello despliega una serie de actividades orientadas a reforzar conocimientos y habilidades generales y/o específicas que ayuden al mejoramiento del desempeño de nuestros colaboradores y a su crecimiento profesional.

5.6. RECURSOS DE COMUNICACIÓN EXISTENTES

En la actualidad la Pontificia Universidad Católica cuenta con los siguientes canales de comunicación formales:

1. Vía Correo Electrónico: Asignado a cada miembro de la Comunidad Universitaria (alumnos, docentes y administrativos).
2. Charlas informativas: Participación de 20 minutos en el proceso de Inducción Institucional y charlas de 60 minutos para las unidades que han pasado una

revisión integral de seguridad de la información según la planificación anual del área.

3. Periódico PUCP: PuntoEDU y sus suplementos, ambos semanales.
4. Revistas PUCP: realizadas en el Fondo Editorial de la Universidad.
5. FanPage en redes sociales de la Universidad y de Facultades.
6. Afiches y paneles: distribuidos en todo el campus universitario.
7. Páginas web: de la PUCP, del Vicerrectorado Académico (Portal VRAC), Vicerrectorado de Investigación (Portal VRI), Vicerrectorado Administrativo (Portal VRAD) y Facultades.

Según la encuesta realizada al personal administrativo y personal docente (ver **ANEXO I**) en la que se les pregunta sobre los canales de comunicación pertinentes para la difusión en seguridad de la información, ambos grupos prefieren la comunicación vía correo electrónico (38% en personal administrativo y 34% en personal académico)

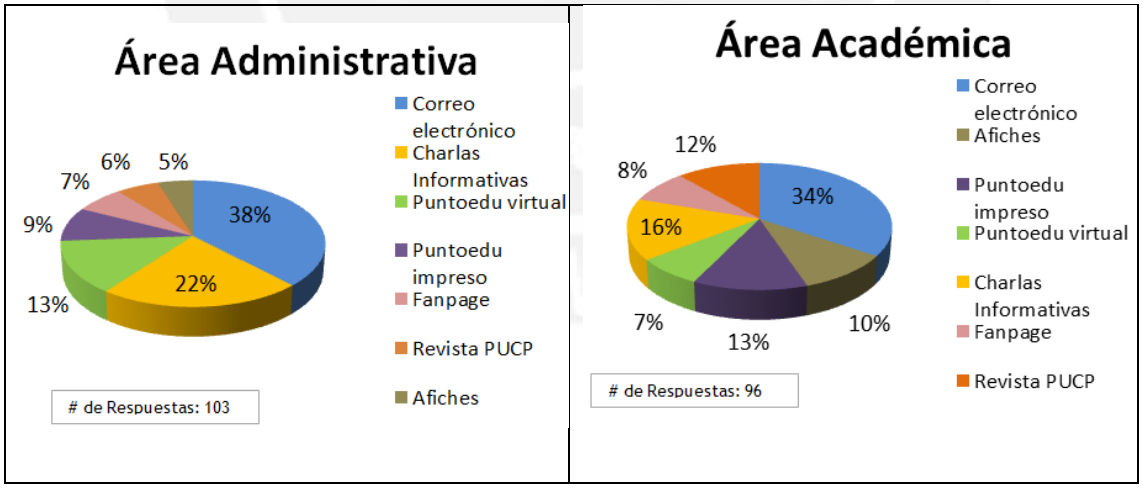


Figura 13 - Preferencias en medios de comunicación por el personal PUCP

CAPÍTULO 2

1. DISEÑO

En este capítulo se presentan los objetivos (generales y específicos), el público primario y públicos secundarios, así como la identificación y priorización de los stakeholders, además se diseña la estrategia y las actividades y productos relacionados con el plan de comunicación.

1.1. OBJETIVOS

Como objetivo principal se define:

Construir para el 2016 las bases para la cultura de seguridad de la información en el personal administrativo de la PUCP a través de concientización del problema, las buenas prácticas en el uso y manejo de la tecnología (entrenamiento) y mediante sus comportamientos (educación) para garantizar la protección y resguardo de la información de la Universidad.

Como objetivos específicos:

ID	OBJETIVOS ESPECÍFICOS
OE01	El personal administrativo de la Universidad conoce y maneja los términos y conceptos básicos en seguridad de la información para el primer semestre del 2016, con la finalidad de crear una estructura base de conocimientos clave para construir la cultura de seguridad de la información en la PUCP
OE02	En el segundo semestre 2016, el personal administrativo conoce los canales de comunicación interna que debe seguir un administrativo PUCP en caso ocurriese un incidente de seguridad de la información.

OE03	El personal administrativo conoce y adepta, durante todo el 2016, un conjunto de buenas prácticas para el personal administrativo, segmentando según las funciones y actividades que realiza.

Tabla 3 - Objetivos Específicos del Plan de Comunicación

1.2. PÚBLICO OBJETIVO

De acuerdo a lo investigado para el presente proyecto, la información obtenida y presentada en el **Capítulo 1 - 4.3. PÚBLICOS**, se estructura a los públicos de la siguiente manera:

1.2.1. Público Primario

Personal Administrativo de la Universidad:

Por brindar el soporte en las funciones, actividades, tareas y proyectos en general de los alumnos y profesores de la Universidad. Además, porque administran y custodian información importante y de soporte para las funciones y procesos de la Universidad (p.e. planilla de la universidad, notas de los alumnos, entre otros).

1.2.2. Públicos Secundarios

Profesores de la Universidad:

Por ser los principales actores de brindar los servicios educativos a los clientes de la Universidad. Todas sus actividades tienen un soporte administrativo, por lo que un

cambio en el personal administrativo se verá reflejado en cierta medida en los profesores (debido a la constante relación laboral que se experimenta entre estos dos públicos).

Tiene además en su poder todos los nuevos conocimientos y de propiedad intelectual de la Universidad.

Estudiantes de la Universidad:

Clientes finales de la Universidad, que reciben el servicio educativo por parte de los profesores y reciben la asistencia administrativa para los otros servicios extra-curriculares a los que acceden durante su vida universitaria.

1.2.3. Identificación y priorización de Stakeholders

Respecto a los Stakeholders del proyecto, se identificó los siguientes:

- Personal Administrativo: Colaboradores PUCP del eje administrativo.

- Profesores con funciones administrativas: Docentes PUCP que ejercen una labor administrativa como parte de sus funciones.

- Investigadores con funciones administrativas: Investigador PUCP que ejerce una labor administrativa como parte de sus funciones.

- Alumnado que realiza prácticas pre-profesionales: Alumnos PUCP que realizan sus prácticas pre-profesionales en una de las unidades de la Universidad.

- Directores Administrativos: Jefes de una Unidad Administrativa. Toda Unidad Administrativa está suscrita al Vicerrectorado Administrativo PUCP.

- Directores Académicos: Jefes de una Unidad Académica (Facultad, Centro o Instituto PUCP). Toda Unidad Académica está suscrita al Vicerrectorado Académico o Vicerrectorado de Investigación.

- Autoridades PUCP: Personas que ejercen un cargo de categoría A dentro de la Universidad y con poder de decisión autónoma. Generalmente son los integrantes de la Asamblea Universitaria o del Consejo Universitario.

- Directores de Unidades que brindan servicios a terceros: La Universidad cuenta con Unidades que se comportan como proveedores de servicios a terceros (Estado Peruano, otras instituciones, entre otros). Como parte de los concursos o licitaciones en las que se participa con el nombre de la Universidad es importante el tema de seguridad de la información.

- DCI: Dirección de Comunicación Institucional, Unidad encargada de todas las comunicaciones transversales para las Unidades PUCP.

- DRH: Dirección de Recursos Humanos, unidad que centraliza los esfuerzos de capacitación y concientización.

A efectos organizativos, se procedió a etiquetar a cada stakeholder:

SH01	SH02	SH03	SH04
Personal Administrativo	Profesores con funciones administrativas	Investigadores con funciones administrativas	Alumnado que realiza prácticas pre-profesionales
SH05	**SH06**	**SH07**	**SH08**
Directores Administrativos	Directores Académicos	Autoridades PUCP	Directores de Unidades que brindan servicios a terceros
	SH09	**SH10**	
	DCI	DRH	

Tabla 4 - Identificación de los Stakeholders del proyecto

1.2.4. Mapeo de Stakeholders

De acuerdo a su nivel de poder, de interés y la posición respecto al proyecto, se mapean a los stakeholders en la **Figura 12**

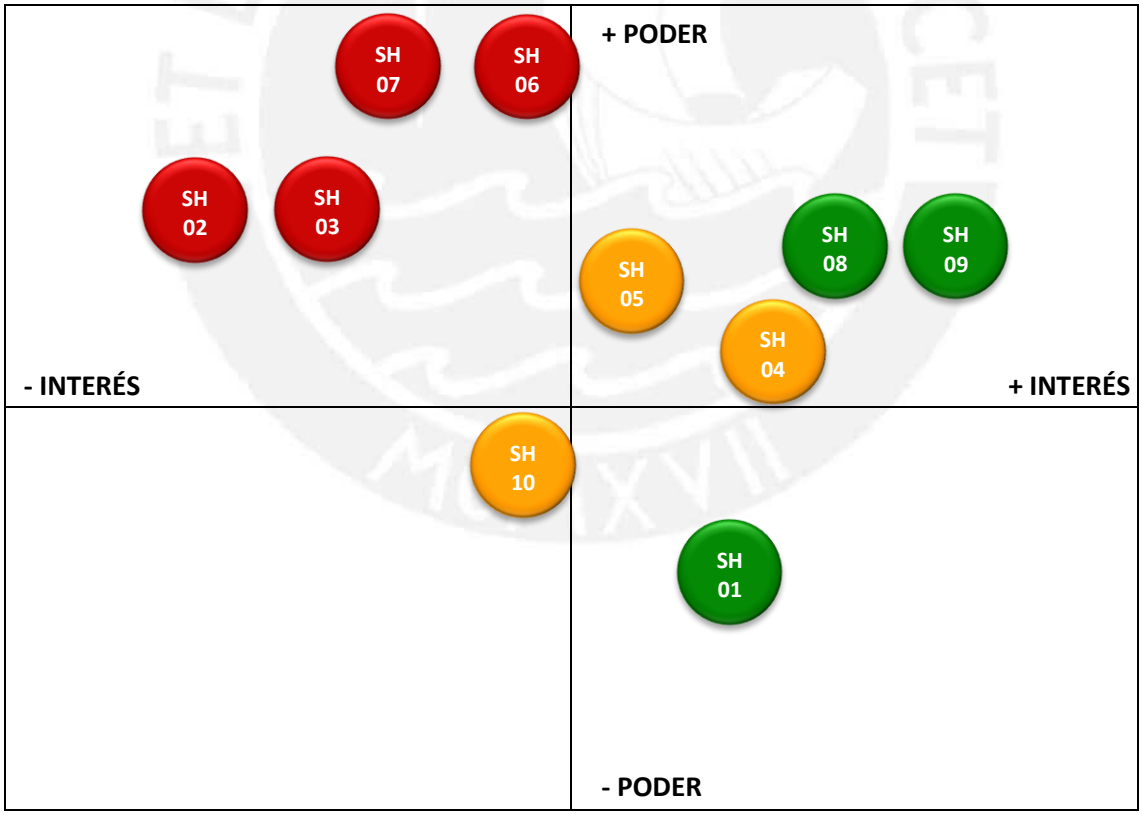


Figura 14 - Mapeo de Stakeholders

1.3. ESTRATEGIAS

Según el modelo de The behaviour change Wheel (Michie, 2011), se propone optar por los siguientes elementos:

Fuentes de comportamiento	Capacidad	De acuerdo a lo recogido en la Encuesta inicial del proyecto (ver **ANEXO 2**)
	Oportunidad	Aplicabilidad hacia la PUCP de la Ley de Protección de Datos Personales
	Motivación	El resguardo de la información no sólo es en el ámbito laboral, aplica también al ámbito personal.
Funciones de intervención	Persuasión	Fase del modelo NIST 108 - **Concientización**
	Capacitación	Fase del modelo NIST 108 – **Entrenamiento**
	Educación	Fase del modelo NIST 108 - **Educación**
Política	Directrices	Existen buenas prácticas internacionales en seguridad de la información.
	Legislación	Aplicabilidad hacia la PUCP de la Ley de Protección de Datos Personales
	Prestación de servicios	La PUCP da y recibe servicios los cuales exigen ciertos niveles de seguridad de la información para concretar dichos convenios.
	Regulación.	La vigencia de la Ley de Delito Informático.

Tabla 5 - Customización del Modelo "The Behaviour Change Wheel" al Proyecto de Comunicación

Como se puede apreciar, las Funciones de Intervención de The behaviour change Wheel hace un cruce alineado con el modelo para la Educación en Seguridad de la Información de la NIST 108. En ese sentido, ambos modelos permitirán un mejor abordaje del objetivo a través del presente proyecto de comunicación.

1.4. ENFOQUES

En base a las conclusiones del problema identificado a través del levantamiento de información y los resultados obtenidos a través de la aplicación de un pre-test (ver **ANEXO V**), se plantea los siguientes enfoques:

ENFOQUE GENÉRICO

La incorporación de hábitos requiere seguir un proceso de incorporación. Es importante que, en un primer momento, el personal administrativo conozca en qué consiste la actividad de seguridad de la información y porqué es relevante que lo incorpore en su día a día. Se ha desarrollado campañas informativas que constará de dos tópicos de información:

- se brinda información sobre la definición de la Seguridad e Información (los pilares, ver Marco Teórico, página 4) a fin que desde un inicio se clarifique el concepto de Seguridad de la Información, los frentes que abarca y la relevancia de uso, ya que en los resultados del diagnóstico se identificó que el público objetivo cuenta en la actualidad con conceptos parciales de la seguridad de la información.
- reforzar el rol del área de Seguridad de la Información como equipo de asesores para la construcción de la cultura de seguridad de la información en la Universidad a través de la capacitación de las personas, ya que es importante fortalecer desde un inicio el reconocimiento del área debido al bajo nivel de conocimiento de la existencia de esta área en la PUCP (resultado del problema identificado).

ENFOQUE PARTICULAR

Un factor clave para la interiorización es el nivel de interés que tienen los participantes para poner en práctica la información brindada, ya que, en caso contrario, sólo se reforzaría el conocimiento general del administrativo y no se garantizaría la ejecución del conocimiento adquirido. Por lo que, el frente de Participación Activa tiene como objetivo definir estrategias basadas en los puntos de interés del público objetivo para que pongan en práctica el conocimiento adquirido.

En base al análisis de los focus grouop (ver **ANEXO V**), se pudo notar que el área administrativa tiene una buena disposición y apertura para la ejecución del Plan de Concientización en Seguridad de Información. Es probable que participen de manera activa en caso se genere competencia y/o reconocimiento de su compromiso hacia la campaña.

Ante contextos diferentes, es importante desarrollar estrategias enfocadas, resaltando los puntos de interés de cada grupo. Mediante este enfoque se desarrollará la rueda "Funciones de Intervención" de The behaviour change Wheel para este proyecto (ver **1.3. ESTRATEGIAS**). En el caso del sector administrativo, es importante desarrollar actividades vinculados a la competencia y reconocimiento para promover su interés y así poco a poco logren interiorizar en su día a día la Seguridad de Información.

POSICIONAMIENTO

Según los resultados del focus group (ver **ANEXO V**), se pudo identificar que la Comunidad Universitaria reacciona a nuevas iniciativas sólo si tienen buen posicionamiento dentro de los medios de comunicación PUCP. Mediante este enfoque se

podrá desplegar la rueda "Políticas" de The behaviour change Wheel para este proyecto (ver **1.3. ESTRATEGIAS**) abordando los temas de buenas prácticas internacionales en seguridad de la información, exponiendo la legislación y reglamentación vigente, entre otros.

Además, este enfoque irá preparando el terreno para la posterior implementación del Comité de Seguridad de la Información, mediante una estrategia de incrementar el nivel de posicionamiento dentro de todos los tópicos que adquiere la Comunidad Universitaria.

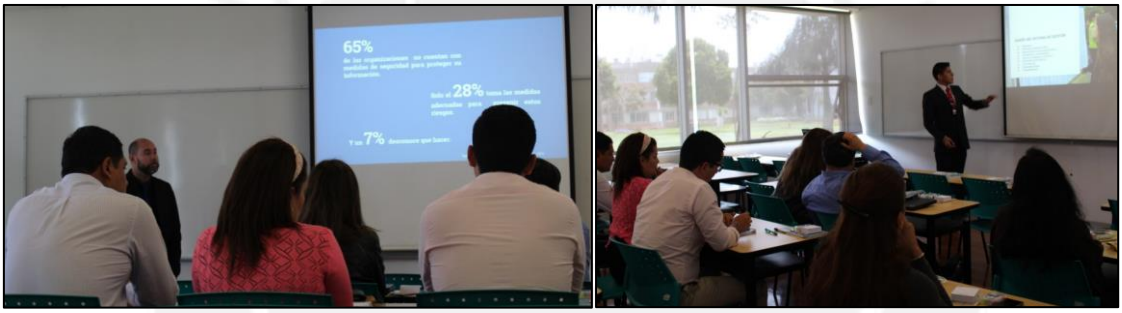
1.5. MENSAJES

Los mensajes a utilizar para el proyecto de comunicación serán los siguientes:

Mensaje	Evidencia
"La PUCP podría ser multada a causa de un mal resguardo de la información"	Multas por no-cumplimiento de la Ley de Protección de Datos Personales hasta las 100UITs (casi S/. 400,000.00)
"Debido a los convenios que tiene la PUCP, se requiere tener un nivel adecuado de seguridad en la información que se maneja"	Si la PUCP no cumple con los estándares de seguridad, podría perder convenios con terceros.
"La seguridad de la información es un asunto, sobretodo, de personas"	Una encuesta realizada a nivel mundial en el 2014 por PwC - PricewaterhouseCoopers evidenció que del total de incidentes de seguridad de la información, un 58% fue por consecuencia de empleados y ex empleados (PricewaterhouseCoopers, 2014).

	Curiosamente, los resultados de la encuesta indican que el número de incidentes reales imputables a los empleados ha aumentado en un 25% desde la encuesta de 2013.
"2 de cada 3 personales PUCP no realiza copias de respaldo de su información"	En la PUCP existe un nivel de riesgo considerable en relación a seguridad de la información según el levantamiento de información que realiza el área de seguridad de la información en las revisiones a las unidades administrativas de la PUCP.

Tabla 6 - Mensajes para el Proyecto de Comunicación



1.6. ACTIVIDADES Y PRODUCTOS

Artículos de Opinión

Mediante publicaciones de contenidos en los medios de comunicación de la PUCP, principalmente en el Punto EDU (impreso y digital) y en el Portal del VRAD (Portal del eje administrativo de la universidad)

Tips en Seguridad de la Información

Animaciones cortas sobre los tips en seguridad de la información (física, digital). Estarían agrupados de la siguiente manera:

Digital	Evite acceder a sitios web de dudosa reputación
	Ignore y no abra correos electrónicos de procedencia dudosa.
	No comparta sus contraseñas con nadie.
	Evite instalar programas o aplicaciones a su computadora.
Físico	Evite imprimir información confidencial a no ser que sea necesario.
	Bloquee su computadora al dejar su puesto de trabajo.
	Guarde su información sensible en un ambiente seguro.
	Destruya documentos impresos que contengan información sensible al botarlos
Generales	Solo comparta información sensible con el personal autorizado.
	Reporte cualquier amenaza a la confidencialidad de su información o la de su oficina

Tabla 7 - Actividades y Productos del Plan de Comunicación

Las plataformas de difusión serían las redes sociales de la PUCP que administra la DCI y las pantallas digitales que se encuentra dentro del campus.

Videos de Concientización

Videos realizados para generar conciencia e iniciar en la cultura de seguridad de la información al personal administrativo. Los videos serán desarrollados en conjunto con la DCI y difundidos en las charlas de capacitación, la página web PUCP y las redes sociales de la universidad.

Pruebas de entrada

Evaluaciones en línea que permitirán crear la línea base sobre el manejo de conocimientos en seguridad de la información que maneja el personal administrativo.

Pruebas de salida

Evaluaciones en línea que permitirán conocer el nivel de manejo de conocimientos en seguridad de la información que maneja el personal administrativo luego de las actividades del presente plan.

Charlas de Concientización

Sesiones de concientización realizadas directamente por el área de seguridad de la información de la Universidad y que están directamente relacionadas con las funciones del área sobre el aseguramiento de las buenas prácticas en las unidades PUCP. Son sesiones de aproximadamente 60 minutos.

Merchandising

Artículos de oficina que incluyen mensajes que incentivan al resguardo de la información que el personal administra.

Activaciones de Seguridad de la Información

Dinámicas de concientización basadas en los juegos y la improvisación con el personal administrativo. Se realiza mediante la ejecución de expertos en activaciones. El objetivo final de estas actividades es lograr la fidelización del personal administrativo con el plan de concientización y sus actividades.

Comité de Seguridad de la Información

Contempla la creación de un grupo del personal administrativo seleccionado por el área de seguridad de la información para cada unidad y que tendrán el rol de "embajadores" y gestores de seguridad de la información, siendo el nexo entre los especialistas y la unidad para consultas, asesorías y atención en caso de incidentes.

2. IMPLEMENTACIÓN

2.1. MATRIZ DE IMPLEMENTACIÓN

De manera holística, para la implementación se considera la siguiente matriz:

Objetivos Específicos			Actividades y/o Productos	Fuentes de Comportamiento			Funciones de Intervención	Políticas			
OE01	OE02	OE03		Capacidad	Oportunidad	Motivación	Fases de la Educación en Seguridad de la Información según NIST 108	Directrices	Legislación	Prestación de servicios	Regulación
P	S		Artículos - Columna de Opinión		✓	✓	Persuasión	✓			
S	S	P	Tips de Seguridad de la Información - RRSS		✓			✓			
S	S	P	Tips de Seguridad de la Información - Pantallas Digitales		✓			✓			
S	S	P	Videos de Concientización			✓		✓			
S		P	Activaciones de Seguridad de la Información	✓		✓		✓	✓		✓
S	S	P	Pruebas de Entrada	✓			Capacitación			✓	
P	S	S	Charlas de Concientización		✓	✓			✓	✓	✓
S	S	P	Pruebas de Salida	✓						✓	
S	P		Entrega de Merchandising			✓		✓			
	P	S	Encuesta final	✓			Educación			✓	

Figura 15 - Actividades y/o Productos del Plan de Comunicación

El detalle de las actividades y sus fechas de ejecución se verán en los siguientes apartados de Cronograma y Presupuestos.

2.2. CRONOGRAMA

El cronograma del Plan de Comunicación propiamente dicho, está desarrollado desde inicios del mes de mayo y se extiende hasta la primera semana de diciembre (culminando con un reporte a los sponsors).

Para efectos visuales, el cronograma ha sido segmentado por semanas, poniendo como rótulo de la semana el primer día (lunes).

Figura 16 - Cronograma del Proyecto de Comunicación

2.3. PRESUPUESTO

El presupuesto ha sido actualizado, debido a que ya no incurrirá en gastos respecto a la implementación y mantenimiento del Club de Seguridad de la Información. Esto reduce el gasto planificado anteriormente inclusive permitiendo que se pueda considerar invertir en el desarrollo de un tercer video de concientización (si así lo requiere el proceso de implementación y de acuerdo al monitoreo del plan).

Además se obtuvo otro ahorro en la realización de videos de concientización (ver detalle en ***3.2. CROWDSOURCING PARA LA IMPLEMENTACIÓN***) lo que permitió considerar el ingreso de las Activaciones de Seguridad de la Información.

Objetivos Específicos			Actividades y/o Productos	PU	Cant.	Total
OE01	OE02	OE03				
P	S		Artículos - Columna de Opinión	S/. -		S/. -
S	S	P	Tips de Seguridad de la Información - RRSS	S/. -		S/. -
S	S	P	Tips de Seguridad de la Información - Pantallas Digitales	S/. -		S/. -
S	S	P	Videos de Concientización	S/. 10,000.00	*2*	S/. 20,000.00
S		P	Activaciones de Seguridad de la Información	S/. 3,000.00	*1*	S/. 3,000.00
S	S	P	Pruebas de Entrada	S/. -		S/. -
P	S	S	Charlas de Concientización	S/. -		S/. -
S	S	P	Pruebas de Salida	S/. -		S/. -
S	P		Entrega de Merchandising	S/. 20.00	*500*	S/. 10,000.00
	P	S	Encuesta final	S/. -		S/. -
			Reportes finales - CISO	S/. -		S/. -
			Reportes finales - Directores	S/. -		S/. -
TOTAL						S/. 33,000.00

Figura 17 - Presupuesto del Plan de Comunicación

2.4. EJECUCIÓN

Al cierre de este informe, estas son las actividades y productos desarrollados según plan:

Artículos de Opinión

En la publicación del PUNTO EDU de 09 de mayo de 2016, se obtuvo desarrollar una columna de opinión sobre seguridad de la información con la finalidad de insertar los tópicos relacionados al universo de temas que presenta este medio de comunicación interno.

SEGURIDAD DE LA INFORMACIÓN

Nuestra información en el correo y redes sociales

Por
MG. LUIS ÁNGEL GUTIÉRREZ
Jefe del área Seguridad de la Información de la Of. de Contraloría

El entorno digital se ha convertido en uno de los 'lugares' en los que se almacena gran cantidad de información de todo tipo: personal, académica, laboral y más. Es en este entorno en el que se encuentran las redes sociales, ya tan familiarizadas con nuestra vida cotidiana, que son una gran vitrina donde muchos de nosotros presentamos nuestro día a día (sin darnos cuenta o no): quiénes somos, qué nos gusta, dónde estuvimos o estaremos, entre muchos otros datos. Por ello, debemos estar al tanto de los riesgos en las redes sociales y las formas de protección que podemos adoptar.

Una de las amenazas en redes sociales y correos electrónicos es el '*phishing*', que consiste en el robo de información mediante la suplantación de una persona u organismo de confianza, que nos ha solicitado datos como contraseñas o claves bancarias por medio de algún correo electrónico o mensaje interno. Otra de las amenazas comunes son los denominados *malware*, que tiene que ver con archivos con fines dañinos o virus que se instalan en nuestra computadora y se dedican a filtrar nuestras contraseñas o algún otro tipo de información confidencial. Finalmente, uno de los riesgos más conocidos y que más se ha incrementado en los últimos años es la suplantación de identidad, que, principalmente, es usada para llevar a cabo actividades ilegales.

Por el bien de nuestra integridad, lo mejor es tener presente cómo protegernos ante las amenazas a la confidencialidad de nuestra información. En ese sentido, podemos tener en cuenta algunas acciones, como evitar abrir correos sospechosos, verificar por otros medios la veracidad esos mensajes y configurar la privacidad de nuestras redes sociales, de forma que limitemos el alcance de la información que publicamos.

El objetivo no es generar una paranoia con relación a cómo administramos nuestra información, sino insertar un criterio de sentido común de la información que compartimos y brindamos, la que usamos y la relevancia de las mismas. Más que preocuparnos en las herramientas, los softwares o las aplicaciones que usaremos para resguardar nuestra información de manera segura, se debe tener en cuenta que la seguridad de la información es un asunto que depende, principalmente, de nosotros mismos, para lo que se necesita sentido común y emplear un buen criterio.

Algunos puntos a tener en cuenta en el correo electrónico y las redes sociales: 1) procura no colocar datos valiosos o íntimos sobre ti; 2) ten cuidado a qué aplicaciones les das tu usuario y tu contraseña; 3) no publiques nada de lo que te tengas que arrepentir; 4) no aceptes correos ni solicitudes de amistad de desconocidos; 5) configura bien las opciones de seguridad y privacidad de las diferentes redes sociales en las que trabajes; 6) haz caso a tu instinto; 7) usa contraseñas seguras y cámbialas cada cierto tiempo; 8) no compartas tus contraseñas con nadie e intenta utilizar claves distintas para las diferentes redes; 9) sé precavido cuando utilices una computadora compartida o pública; 10) no confíes en todo lo que se dice en internet (loterías, premios, solicitudes de amistad, descuentos, correos, pedidos de ayuda, etc.). ■

En la publicación del PUNTO EDU de 12 de setiembre de 2016, se mantuvo la aparición de la Columna de Opinión respecto a temas de seguridad de la información. Además se obtuvo un compromiso bidireccional con la Dirección de Comunicación Institucional para tener presencia mensual en la sección de Opinión del Punto EDU.

PROTECCIÓN DE DATOS

Por
ING. FERNANDO HUAMÁN MONZÓN
Analista de Seguridad de la Información de la Oficina de Contraloría

Nuestra privacidad, un punto importante

Hace unas semanas WhatsApp -propiedad de Facebook desde el 2014- anunció un cambio en sus términos de uso y política de privacidad que contempla el intercambio de información entre dicha aplicación y la red social mencionada. ¿En qué me puede afectar el cambio de la política de privacidad de una aplicación o servicio que uso? O mejor aún ¿quién lee las políticas de uso y privacidad? Lamentablemente, no hay respuesta, solo podemos decir que todos, o casi todos, hacemos clic en "Aceptar" sin dudar y no leemos dichas políticas.

Gmail, por ejemplo, cuenta con más de 16 páginas de términos y condiciones de uso y privacidad, sin embargo, pocos hemos leído las implicancias que designa el correo de Google hacia nuestra privacidad. ¿Quién podría imaginarse que nuestra aplicación de línterna recopila información de geolocalización para fines de publicidad? Este detalle se encuentra en los términos de Condiciones de uso y privacidad.

El tema de las políticas de privacidad lleva ya un buen camino recorrido, en el 2005, la empresa PC Pitstop determinó, en sus Términos y Condiciones de Uso, que regalaría US$ 1,000 al primero que leyera su política y llamara a la empresa. Luego de cuatro meses hubo un feliz ganador de este experimento.

De la misma manera, nuestra Universidad cuenta con una Política de Privacidad que es importante que toda la comunidad universitaria y personas (naturales y jurídicas) que se relacionan con ella la conozcan. En ella, se menciona el compromiso de la PUCP con la protección de datos personales y las directrices sobre la confidencialidad de la información que administra la Universidad. Además, se especifican los tipos de tratamiento que se darán a los datos personales de alumnos y egresados, de nuestros profesores, de nuestros colaboradores, de las personas que postulan a una oportunidad de docencia en la PUCP, de los postulantes de pregrado y posgrado, de los alumnos de formación continua, y de otras actividades académicas y no académicas.

Todo ello responde, además, a la aplicación de la Ley 29733 – Ley de Protección de Datos Personales, que se encuentra vigente desde el 8 de mayo de 2015, que pretende velar por el derecho fundamental que tiene toda persona de controlar su información personal que comparte con terceros, así como el derecho a que esta se utilice de forma apropiada, es decir, de forma que no la perjudique.

Al tener en claro que las Políticas de Privacidad son una declaración de la empresa u organización sobre cómo va a administrar los datos que otorgamos en la interacción con su producto o servicio, es importante que entendamos la privacidad como nuestro derecho fundamental y que, por lo tanto, debe ser respetado. Recordemos que la responsabilidad de administrar datos personales empieza por nosotros mismos desde nuestro interés de protegerlos. ■

Así mismo, en la publicación del PUNTO EDU de 24 de octubre de 2016, se mantuvo la aparición de la Columna de Opinión respecto a temas de seguridad de la información, teniendo además presencia en la web de la PUCP (http://puntoedu.pucp.edu.pe/opinion/algunos-detalles-al-pasar-la-tarjeta/).

EVITA LOS FRAUDES

ILUSTRACIONES: GABRIELA LAYZA

Por
ING. FERNANDO HUAMÁN
Analista de Seguridad de la Información de la Oficina de Contraloría

Algunos detalles al "pasar la tarjeta"

En el Perú existen alrededor de 21 millones de tarjetas de débito y más de 8 millones de tarjetas de crédito, según Asbanc, al cierre de agosto de este año (esta cantidad no incluye tarjetas adicionales). Existen varios temas a los cuales brindarles prioridad respecto a las tarjetas de crédito, uno de ellos es el preocupante comportamiento de los peruanos en su uso, por ejemplo, el 33.3% de la población las usa para disposición en efectivo (una de las opciones de financiamiento más caras en el sistema financiero); otro tema es la seguridad al usar las tarjetas de crédito y débito, pues es aquí donde se generan muchos problemas. A continuación, algunos alcances sobre este importante tema.

Al hacer uso de nuestras tarjetas, solemos hacerlo por comercio electrónico o para pagar en establecimientos donde hemos recibido un servicio o comprado un producto. Una de las situaciones más frecuentes es cuando hacemos uso de nuestra tarjeta de crédito -o débito- para comercio electrónico, es decir la compra de algún producto vía página web o la transacción de dinero. En este caso, la medida de prevención que podemos adoptar es la comprobación de la URL del sitio. Para esto, los navegadores ya cuentan con la verificación de las páginas mediante certificados digitales: elementos de seguridad que expide un tercero garantizando que la web es de la entidad que dice ser. Mucho mejor, ahora los navegadores muestran visualmente, mediante colores, candados u otra simbología, la legitimidad de la URL, así nos aseguramos que estamos en la web correcta.

> "SI TU TARJETA VENCIÓ, SE DETERIORÓ O LA HAS CANCELADO, DESTRÚYELA RASPANDO LA FIRMA Y CORTANDO EL PLÁSTICO".

Pero, ¿qué hacemos si el navegador no pudo verificar la legitimidad de la URL? Eso no quiere decir que la URL es falsa, necesariamente, pues podría ser que no cuenta con su certificado digital. Para hacer más explícita esta situación, podríamos tomar el ejemplo de una intervención policial, si fuéramos detenidos y no contáramos con nuestro documento de identidad, no significa que no seamos quien decimos ser, solo que el agente policial no tendría ningún documento que le permita comprobarlo.

Para evitar situaciones desafortunadas, lo primero que podemos hacer es escribir directamente la URL en el navegador, en lugar de llegar a ella dando clic desde un enlace de correo u otra página web. Luego, Firefox, Chrome y Safari cuentan con herramientas antifraude, es importante habilitarlas pues tienen registros de webs notificadas como fraudulentas.

Por otro lado, al "pasar la tarjeta", es decir pagar un servicio o producto desde nuestra tarjeta, de crédito o débito, también debemos tener en cuenta ciertas medidas de seguridad.

Una de las medidas más sencillas y eficaces que podemos implementar es firmar nuestra tarjeta y verificar frecuentemente que la tarjeta que portamos corresponde a la nuestra. Al realizar los pagos nunca perdamos de vista nuestra tarjeta y que la transacción siempre se haga en nuestra presencia. Si vas a salir a almorzar o hacer compras, solo lleva lo necesario: identificación y las tarjetas de crédito o débito que vas a utilizar. No prestes tu tarjeta, ni permita que otras personas la usen en su nombre. Y si tu tarjeta venció, se deterioró o la has cancelado, destrúyela raspando la firma y cortando el plástico en fragmentos.

Si bien debemos de ser conscientes de que la seguridad de nuestras tarjetas de crédito está en nosotros como dueños de la misma, también existe responsabilidad de seguridad en los establecimientos donde realizamos nuestras transacciones. Para ello, es importante tener la confianza en qué lugares usamos nuestras tarjetas de crédito y débito.

En ese sentido, en la PUCP se están realizando los esfuerzos necesarios (mediante la Oficina de Contraloría, Dirección de Tecnologías de Información y la Oficina de Tesorería) para que los procesos, tecnologías y personal de la Universidad estén adecuados a la norma PCI-DSS, la cual brinda unos estándares de seguridad de la información en flujos de datos de tarjetas. Este esfuerzo que se viene realizando le brindará, al módulo de pago electrónico mediante Campus Virtual y los puntos de caja de la Universidad, los niveles de seguridad de la información adecuados para que las transacciones que se realicen a través de ellas estén reguardadas y seguras.

Recuerda que el cuidado y seguridad de tu tarjeta depende sobre todo de la aplicación de buenas prácticas. ■

puntoedu.pucp.edu.pe/opinion/algunos-detalles-al-pasar-la-tarjeta/

INSTITUCIONALES | INVESTIGACIÓN | AGENDA | PRENSA

Opinión

24 de octubre del 2016

Algunos detalles al "pasar la tarjeta"

Fernando Huamán
Analista de Seguridad de la Información de la Oficina de Contraloría

Me gusta
Twittear
G+1
Compartir
Imprimir
PDF
Correo electrónico

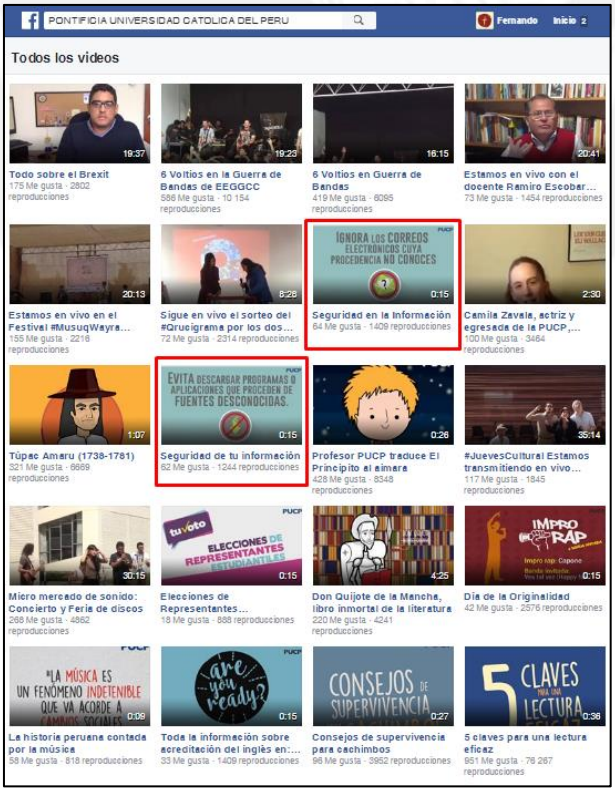
"Si tu tarjeta venció, se deterioró o la has cancelado,

En el Perú existen alrededor de 21 millones de tarjetas de débito y más de 8 millones de tarjetas de crédito, según Asbanc, al cierre de agosto de este año (esta cantidad no incluye tarjetas adicionales). Existen varios temas a los cuales brindarles prioridad respecto a las tarjetas de crédito, uno de

Como parte del Enfoque de Posicionamiento (ver **1.4. ENFOQUES**) la presencia también se replicó en los portales relacionados al personal administrativo:

Tips en Seguridad de la Información

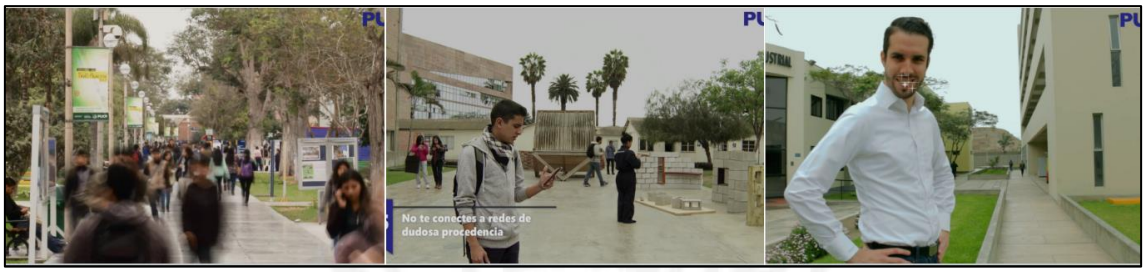
Mensualmente se viene publicando (a través de las redes sociales PUCP administradas por la DCI y en las pantallas digitales en el campus) los tips de seguridad de la información desarrollados por el área de Animaciones de la Dirección de Comunicación Institucional.



Videos de Concientización

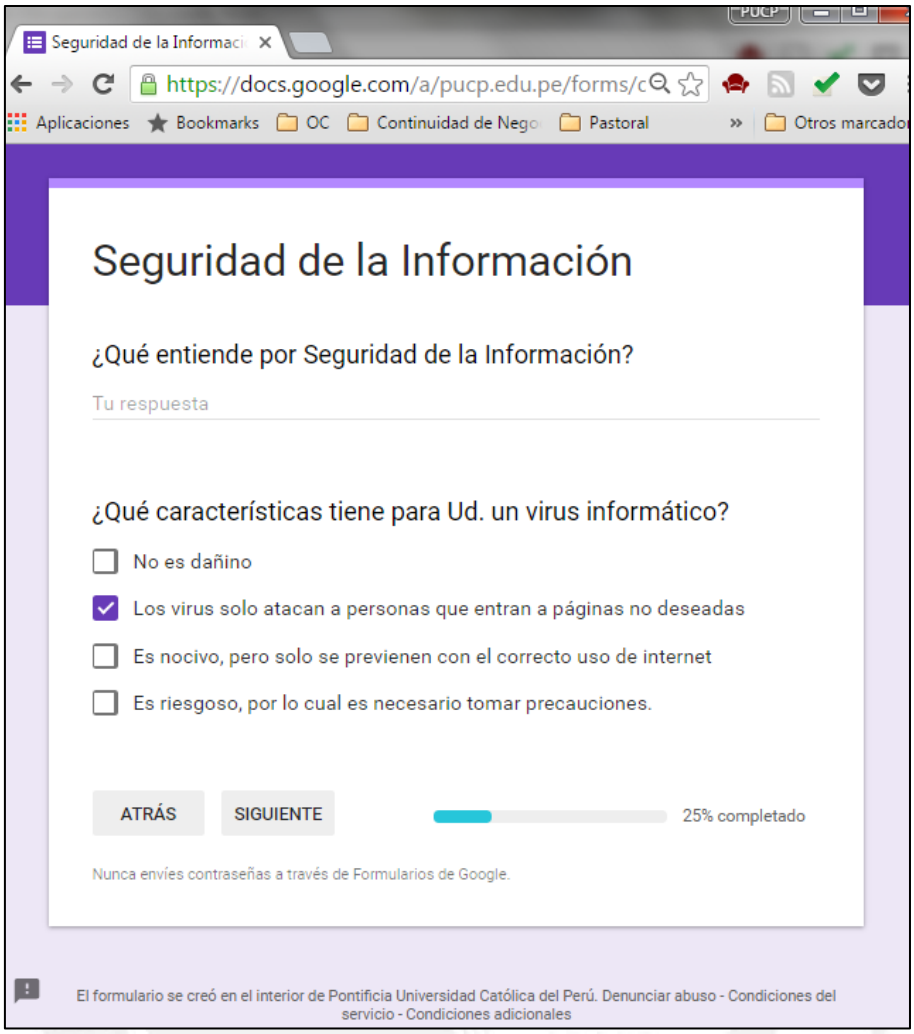
Desde el 24 de mayo se tiene disponible el video desarrollado por una empresa audiovisual sobre la concientización en seguridad de la información.

Además, gracias a la implementación de Crowdsourcing en el proyecto de comunicación se viene elaborando videos de concientización desarrollados por los alumnos de un curso de producción audiovisual de la Facultad de Ciencias y Artes de la Comunicación. El detalle puede verse en punto ***3.2. CROWDSOURCING PARA LA IMPLEMENTACIÓN.***



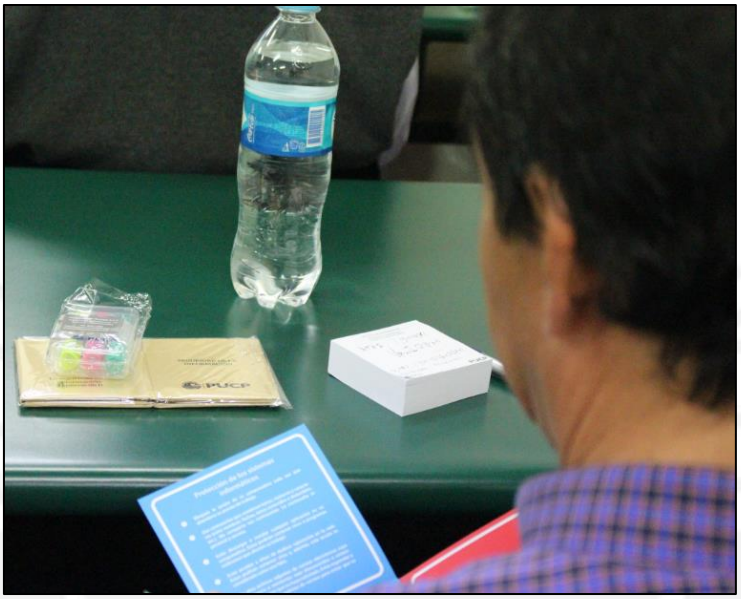
Pruebas de entrada/salida

Evaluaciones en línea que permitirán crear la línea base sobre el manejo de conocimientos en seguridad de la información que maneja el personal administrativo, así como la interiorización de los conceptos de seguridad de la información brindados en las Charlas de Concientización. Se desplegó en 3 unidades: CeprePUC, Oficina Central de Admisión e Informes y Oficina de Tesorería (responsables de puntos de caja)



Charlas de Concientización

Sesiones de concientización realizadas directamente por el área de seguridad de la información de la Universidad y que están directamente relacionadas con las funciones del área sobre el aseguramiento de las buenas prácticas en las unidades PUCP. Son sesiones de aproximadamente 60 minutos.



Merchandising

Artículos de oficina que incluyen mensajes que incentivan al resguardo de la información que el personal administra. Se aumentaron 03 artículos más al kit de seguridad de la información: portalapiceros, tacos de papel y resaltadores.

Además, como parte del Plan de Comunicación se replanteó la línea gráfica de Seguridad de la Información luego de una validación de colores quedando la siguiente actualización: Paleta de colores verde limón, verde agua, celeste que refleja una combinación acorde con la tecnología y la modernidad, (en la Universidad se usa mucho el azul oscuro que hace que las piezas sean más serias e institucionales). Esta nueva combinación es mucho más joven, divertida, moderna y amigable.

Comité de Seguridad de la Información

Aún no se ha ejecutado y ha sufrido un replanteamiento, debido a que inicialmente se formuló en la implementación y mantenimiento como parte de este plan de comunicación, sin embargo, previa a su implementación era necesario crear las bases (tanto en motivación como en oportunidad, ver **1.3. ESTRATEGIAS**) para estos fines. Este plan de comunicación proveerá los cimientos para la implantación del Comité de Seguridad de la Información que será comentado en el punto **6. RECOMENDACIONES**.

Activaciones de Seguridad de la Información

Gracias al ahorro en recursos económicos que se pudo obtener por el monitoreo del proyecto a partir de la ejecución de Crowdsourcing (ver **3.2. CROWDSOURCING PARA LA IMPLEMENTACIÓN**) se pudo optar, en el transcurso del desarrollo del plan, la ejecución de activaciones de seguridad de la información.

2.5. OBSERVACIONES

Uno de los inconvenientes que se presentaron fue en el desarrollo de productos realizado por terceros, pues al tratarse de un outsourcing fuera del ámbito académico, no se consideraron las validaciones previas a la versión final del producto y se basaron únicamente en la experiencia y conocimiento que tiene el proveedor (interno) sobre el público al cual está dirigido este plan. En próximas coordinaciones se especificarán claramente la exigencia de este paso.

Dentro de las actividades que permitan un mejor control del plan, se propone llevar en paralelo una gestión del conocimiento del plan de comunicación. Esta Gestión brindará

inputs tanto para la mejora de este plan de comunicación y posteriores planes que pretendan atender la continuación del presente plan o uno similar. Para las próximas actividades se planteará la incorporación de este factor.

3. MONITOREO Y EVALUACIÓN

3.1. MODELO DE GESTIÓN PARA EL MONITOREO

De acuerdo a la Herramienta de Gestión: ***Puntos de Tracción*** o ***Quick Wins*** se adaptó para el proyecto de implementación trazando vínculos de acuerdo a:

- ✓ Dependencia de recursos (económicos, tiempo) para el desarrollo o ejecución.
- ✓ Autonomía parcial del desarrollo o ejecución
- ✓ Autonomía total para el desarrollo o ejecución

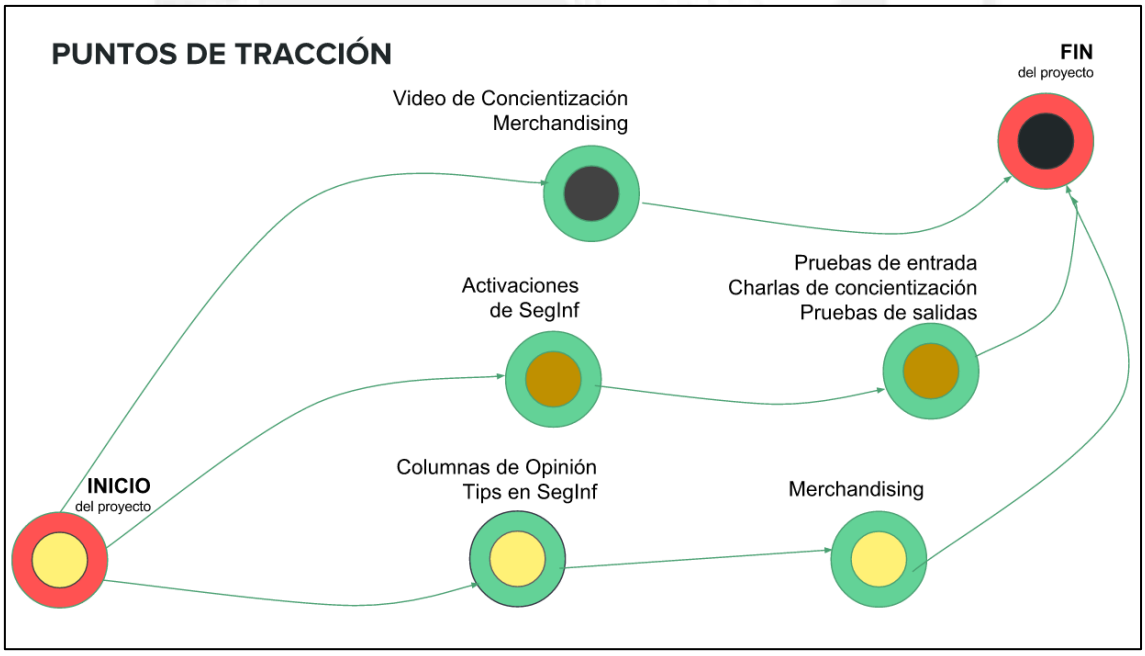


Figura 18 - Modelo Monitoreo para el Plan de Comunicación

Se optó por tener un factor de dependencia debido al mayor riesgo que tienen los proyectos de implementación que es en relación a la asignación de recursos y tiempos (coordinación con terceros) como se puede ver en la **Figura 18**.

Las Columnas de Opinión, los tips de Seguridad de la Información y el stock de Merchandising con la que cuenta el área de seguridad de la información están en total administración y bajo la responsabilidad de los mismos responsables de la ejecución del proyecto. Por lo tanto existe una Autonomía total para el desarrollo o ejecución de estas actividades.

Las Activaciones de Seguridad de la Información, las pruebas de Entrada, las Charlas de Concientización y las Pruebas de Salida han sido coordinadas con las unidades a las cuales está enfocada. Por lo tanto existe una Autonomía parcial del desarrollo o ejecución de estas actividades.

La realización de los videos de concientización y de adquisición de nuevo merchandising está en dependencia de la asignación de recursos económicos para su desarrollo o ejecución.

Cada una de estas líneas de acción han sido monitoreadas de diferente manera por su naturaleza de dependencia.

3.2. CROWDSOURCING PARA LA IMPLEMENTACIÓN

Al tener identificado el mayor riesgo que tienen los proyectos de implementación que es la asignación de recursos y tiempos (coordinación con terceros), se propuso además tener en constante revisión las oportunidades de generar modelos de sostenibilidad mediante el Crowdsourcing.

3.2.1. Modelo de Crowdsourcing para el proyecto

Adecuando al contexto del proyecto, se propuso el siguiente modelo de sostenibilidad

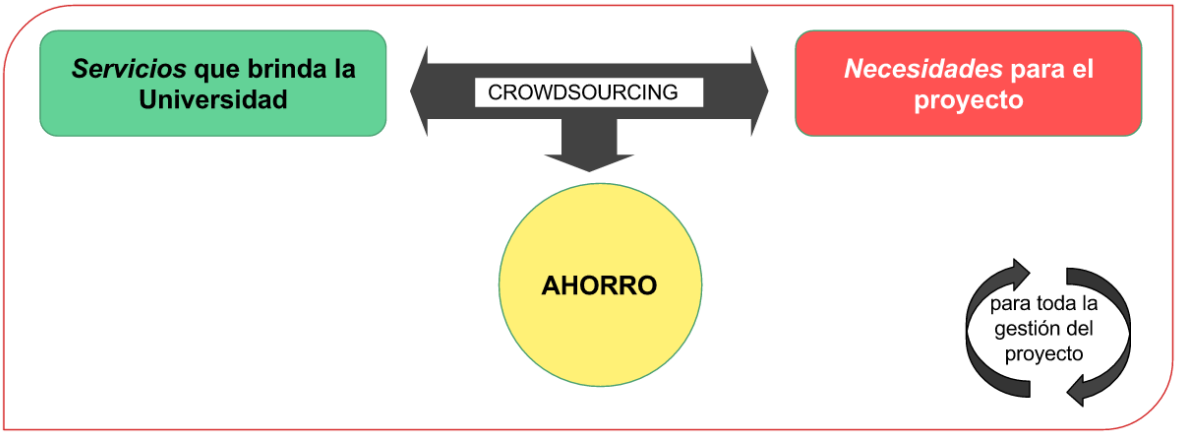


Figura 19 - Modelo de Crowdsourcing para el Proyecto de Comunicación

Para todos los servicios que brinda la Universidad (sobre todo enfocados en los cursos de los planes de estudios de las diversas carreras) se puede relacionar con una de las necesidades que tenga el proyecto. Su enlace de un servicio de la Universidad con una necesidad del proyecto provocaría un ahorro en costos. Este monitoreo debe realizarse para toda la gestión del proyecto con la finalidad de encontrar la oportunidad de ejecutar crowdsourcing a favor del proyecto.

3.2.2. Caso de implementación: Videos de concientización

Para la necesidad de desarrollar videos de concientización de seguridad de la información, se pudo coordinar con la Facultad de Ciencias y Artes de la Comunicación para que como parte de un trabajo del semestre de un curso de producción audiovisual, se puedan generar estos videos de concientización.

La cotización de un video de concientización hubiera costado alrededor de 3,000 soles. La producción de un video con las mismas características desde el modelo de Crowdsourcing a través de la Facultad (servicio de la misma Universidad) sólo costó 500 soles en la asignación de movilidad y gastos generales para los alumnos de ese curso.

4. RESULTADOS

4.1.1. Inventario de indicadores

Los indicadores son una herramienta de control de gestión que permite medir de manera objetiva el cumplimiento del objetivo general de un proyecto. Con la finalidad de realizar un adecuado seguimiento del Plan de Comunicación en seguridad de información, se ha identificado los siguientes indicadores:

ACTIVIDADES Y/O PRODUCTOS	INDICADORES	INSTRUMENTO DE MONITOREO
Artículos - Columna de Opinión	Métricas de DCI de la operatividad de la difusión. (evaluación de la campaña de difusión en base a indicadores como recordación de los mensajes, efectividad de las acciones realizada, y opinión acerca de la estrategia utilizada.)	Plataforma de la DCI de medición de analítica web (página web, youtube y facebook). Registro en programación DCI para la difusión en pantallas digitales.
Tips de Seguridad de la Información - RRSS		
Tips de Seguridad de la Información - Pantallas Digitales		
Videos de Concientización		

ACTIVIDADES Y/O PRODUCTOS	INDICADORES	INSTRUMENTO DE MONITOREO
Activaciones de Seguridad de la Información	Porcentaje de aceptación de la actividad por parte de los colaboradores	*Encuestas virtuales del área de seguridad de la información*
Pruebas de Entrada/Salida	*Cantidad de conceptos de seguridad de la información interiorizados por el personal*	*Encuestas virtuales del área de seguridad de la información*
Charlas de Concientización	*Cantidad de personas participantes.*	*Control de asistencia a charlas de capacitación*
Merchandising	Percepción de merchandising en los colaboradores.	Encuestas virtuales del área de seguridad de la información
Encuesta final	Reducción del 25% de malas prácticas en seguridad de la información	Evaluaciones del área de seguridad de la información a las unidades
Reportes finales - CISO	Presupuesto Programado/Presupuesto Ejecutado	Análisis presupuestario del plan (modificado y ejecutado)
Reportes finales - Directores		

Tabla 8 - Inventario de Indicadores del Plan de Comunicación

El análisis de indicadores permite obtener una visión más específica de los avances. En base a los resultados se realizan planes de acción o modificaciones para garantizar el cumplimiento del Plan de Comunicación.

4.1.2. Resultados de indicadores del Proyecto

Finalizadas las actividades de implementación y a la fecha de entrega del presente informe se obtuvieron los siguientes resultados:

ACTIVIDADES Y/O PRODUCTOS	INDICADORES	INSTRUMENTO DE MONITOREO	INICIAL	META	FINAL	EFECTIVIDAD
Artículos - Columna de Opinión	Métricas de DCI de la operatividad de la difusión. (evaluación de la campaña de difusión en base a indicadores como recordación de los mensajes, efectividad de las acciones realizada, y opinión acerca de la estrategia utilizada.)	Plataforma de la DCI de medición de analítica web (página web, youtube y facebook). Registro en programación DCI para la difusión en pantallas digitales.	N.A	4 artículos	3 artículos	75.00%
Tips de Seguridad de la Información - RRSS			N.A	1,500 vistas/tip	1,370.5 vistas/tip	91.37%
Tips de Seguridad de la Información - Pantallas Digitales			N.A	56 vistas/día	56 vistas/día	100.00%
Videos de Concientización			N.A	1,000 rep. al finalizar el proyecto	858 rep. al finalizar el proyecto	85.80%
Activaciones de Seguridad de la Información	Porcentaje de aceptación de la actividad por parte de los colaboradores	*Encuestas virtuales del área de seguridad de la información*	N.A	75% aceptación	76.9% aceptación	**102.53%**
Pruebas de Entrada/Salida	*Cantidad de conceptos de seguridad de la información interiorizados por el personal*	*Encuestas virtuales del área de seguridad de la información*	10 de 20 conceptos	15 de 20 conceptos	15 de conceptos	100.00%
Charlas de Concientización	*Cantidad de personas participantes.*	*Control de asistencia a charlas de capacitación*	N.A	3 áreas (112 colaboradores)	3 áreas (87 colaboradores)	77.68%
Merchandising	Percepción de merchandising en los colaboradores.	Encuestas virtuales del área de seguridad de la información	N.A	75% de buena percepción	82.05% de buena percepción	**109.40%**
Encuesta final	Reducción del 25% de malas prácticas en seguridad de la información	Evaluaciones del área de seguridad de la información a las unidades	16 malas prácticas	12 malas prácticas	13 malas prácticas	75.00%

ACTIVIDADES Y/O PRODUCTOS	INDICADORES	INSTRUMENTO DE MONITOREO	INICIAL	META	FINAL	EFECTIVIDAD
Reportes finales - CISO	Presupuesto Programado/Presupuesto Ejecutado	Análisis presupuestario del plan (modificado y ejecutado)	S/. 33,000.00	S/. 33,000.00	S/. 23,000.00	**143.48%**
Reportes finales - Directores						

5. CONCLUSIONES

5.1. Sobre la estrategia del Plan de Comunicación

El personal administrativo conoce y maneja, en un 50% más, los conceptos básicos en seguridad de la información logrando el objetivo al 100% respecto al Objetivo Específico 01, lo que permite el inicio de la estructura base de conocimientos clave para construir la cultura de seguridad de la información en la PUCP.

Un 72% más de los colaboradores reconoce los canales de comunicación interna que debe seguir un administrativo PUCP en caso ocurriese un incidente de seguridad de la información (contactarse con la Dirección de Tecnologías de Información o el área de Seguridad de la Información de la Universidad).

Un 37% más del personal administrativo conoce y adopta un conjunto de buenas prácticas para el personal administrativo, segmentando según las funciones y actividades que realiza. Esto se pudo verificar con las revisiones nocturnas realizadas a las Unidades.

5.2. Sobre los mensajes y las actividades y productos

La selección de 4 mensajes claves a efectos del Plan de Comunicaciones en Seguridad de la Información permitió la consecución de los objetivos de manera satisfactoria (ver **4.1.2. Resultados de indicadores del Proyecto**) esto fue gracias al aporte de The behaviour change Wheel, en sus Políticas y Funciones de Intervención.

5.3. Sobre la gestión del proyecto

La implementación de herramientas de la Ciencias de la Gestión en el proyecto permitió mejoras considerables al mismo. Gracias a los modelos de Crowdsourcing (ver **3.2.1. Modelo de Crowdsourcing para el proyecto**) y de Puntos de Tracción o QuickWins (ver **3.1. MODELO DE GESTIÓN PARA EL MONITOREO**), se pudo lograr un ahorro del 30.30% del presupuesto inicial para el proyecto.

6. RECOMENDACIONES

Como se presentó en **2.1. MATRIZ DE IMPLEMENTACIÓN** y de acuerdo al modelo NIST 108 para la Educación en Seguridad de la Información (ver **Figura 3 - Educación en Seguridad de la Información**), se recomienda continuar con esta implementación para abordar en mayor medida la fase de Educación del modelo NIST 108. El presente proyecto de comunicación permitió tener las bases para construir la cultura de seguridad de la información en el personal administrativo de la Universidad mediante un enfoque

que se concentró en mayor medida en las fases Concientización y Entrenamiento del modelo NIST 108.

Debido al aporte en el éxito del presente proyecto de comunicación, se recomienda poner mayor énfasis en futuros esfuerzos comunicacionales las herramientas aplicables desde las Ciencias de la Gestión, como fue el caso de los modelos Crowdsourcing y Puntos de Tracción (ver **3.2.1. Modelo de Crowdsourcing para el proyecto** y **3.1. MODELO DE GESTIÓN PARA EL MONITOREO**)

BIBLIOGRAFÍA

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review*, 191-215.

da Veiga, A., & Martins, N. (2015). *Improving the information security culture through monitoring and implementation actions illustrated through a case study.*

Herold, R. (2005). *Information security and privacy awareness program.* Estados Unidos: Auerbach Publications.

ISACA. (2010). *The Business Model for Information Security.* Estados Unidos.

ISACA. (2011). *Creating a Culture of Security.* Estados Unidos.

ISACA. (2012). *COBIT® 5 para Seguridad de la Información.* Estados Unidos.

ISO - International Organization for Standardization. (2009). *Information technology - Security techniques - Information security management systems - Overview and vocabulary.* Suiza: ISO.

Michie, S. (2011). The behaviour change wheel: A new method for characterising and designing behaviour change interventions. *Implementation Science*, 42.

NIST. (08 de 10 de 2015). *NIST Special Publication 800-16.* Obtenido de Computer Security Resource Center: http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf

Ponemon Institute. (2013). *2013 Cost of Data Breach Study: Global Analysis.*

Pontificia Universidad Católica del Perú. (2014). *Estatuto.*

PricewaterhouseCoopers. (2014). *The Global State of Information Security.*

Prochaska, J., & Diclemente, C. (1983). Stages and processes of self-change in smoking: Toward an integrative model of change. *Journal of Consulting and Clinical Psychology*, 51, 390-395.

PwC. (2016). *Price waterhouse Cooper.* Obtenido de http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html

Shannon, C., & Weaver, W. (1981). *Teoría matemática de la comunicación.* Madrid: Ediciones Forja.

Tuck School of Business at Dartmouth. (2011). *Tuck School of Business at Dartmouth* . Obtenido de http://exec.tuck.dartmouth.edu/downloads/623/human_behavior_and_security_culture_ciso_workshop_overview.pdf

Tupia, M. (2010). *Administración de la seguridad de información.* Perú: Graficar.

ANEXO I

8 COMPORTAMIENTOS IDEALES PARA LA CULTURA EN SEGURIDAD DE LA INFORMACIÓN

Comportamiento	Descripción
1. La seguridad de la información se practica en las operaciones diarias	La seguridad de la información es parte del funcionamiento diario de la empresa. A nivel organizativo, el comportamiento indica que la seguridad de la información se acepta como un imperativo empresarial en el establecimiento de los objetivos organizativos. A nivel individual, esto significa que a los individuos les importa el bienestar de la empresa y por lo tanto aplican técnicas de seguridad de la información y un enfoque de prudencia en sus operaciones cotidianas.
2. Las personas respetan la importancia de las políticas y principios de la seguridad de la información.	El personal de la empresa reconoce la importancia de las políticas y principios de la seguridad de la información. A nivel organizativo, la alta dirección respalda las políticas y principios aprobándolas, revisándolas y comunicándolas de manera regular. A nivel individual, los empleados han leído y comprendido las políticas, y se sienten capacitados para seguir las directivas de la empresa.
3. Las personas poseen un nivel detallado y suficiente de orientación en seguridad de la información y se les anima a participar y cuestionar la situación actual de seguridad de la información	Las personas poseen un nivel detallado y suficiente de orientación en seguridad de la información y se les anima a participar y cuestionar la situación actual de seguridad de la información en dos niveles. La cultura organizativa indica un proceso de comunicación de dos vías para la orientación y para la retroalimentación y proporciona a las partes interesadas una oportunidad para realizar comentarios sobre los cambios; la cultura individual demuestra la participación de las partes interesadas cuestionando y proporcionando comentarios cuando se les solicita.
4. Todo el personal es responsable de que se proteja la información de la empresa.	Esta responsabilidad se refleja en dos niveles dentro de la empresa. En el nivel organizativo, se hacen constar aquellas incidencias que impliquen responsabilidades (disciplina), y se confirman los roles de las partes interesadas relativos a su aplicación. En el nivel individual se requiere a cada individuo que comprenda las responsabilidades asumidas relativas a la seguridad de la información.

5. Las Partes Interesadas están informadas de cómo identificar y responder a las amenazas en el contexto de la empresa.	Se pueden implementar los procesos adecuados para identificar y responder a las amenazas a nivel organizativo mediante la instauración de un proceso de notificación de incidencias y de un proceso para minimizar las pérdidas de información. A nivel individual, el personal debe estar formado sobre qué constituye un incidente de seguridad, cómo se debe notificar sobre él y cómo reaccionar.
6. La Dirección respalda y anticipa las innovaciones en seguridad de la información de manera proactiva y lo comunica a toda la empresa. La empresa es receptiva para tener en cuenta y manejar nuevos retos en materia de seguridad de la información.	Las innovaciones y retos en seguridad de la información se abordan a nivel organizativo mediante un equipo de investigación y desarrollo en seguridad de la información. La cultura individual contribuye con las partes interesadas para aportar nuevas ideas.
7. La Dirección de negocio se compromete a colaborar transversalmente de manera continuada para conseguir programas de seguridad de la información efectivos y eficientes.	La colaboración multifuncional se alcanza mediante la aceptación por parte de la organización de una estrategia de seguridad de la información con un enfoque holístico y a través de una integración mejorada con el negocio. Los individuos contribuyen a través del acercamiento a otras funciones de negocio y mediante la identificación de posibles sinergias.
8. La alta dirección reconoce el valor para el negocio de la seguridad de la información.	El valor para el negocio de la seguridad de la información se reconoce a nivel organizativo en cuanto la seguridad de la información se ve como un medio para mejorar el valor del negocio (beneficio, coste, reputación y ventaja competitiva), la transparencia en la respuesta a las incidencias es clave y se considera esencial comprender las expectativas de los clientes. A nivel individual, este comportamiento se pone de manifiesto con la generación de ideas creativas que generan valor (a varios niveles dentro de la seguridad de la información).

Tabla 9 - Comportamientos ideales propuesto por ISACA para la Cultura en Seguridad de la Información.

ANEXO II
ENCUESTA DE DIAGNÓSTICO

La población de la PUCP es de 6687 colaboradores (3321 administrativos y 3366 docentes) al 1 de abril de 2016. Se consideró tomar como muestra el 2% de cada área (70 participantes aproximadamente).

Con el fin de tener una idea general de la percepción de los colaboradores de la PUCP sobre Seguridad de la Información, se procedió a enviar la encuesta elaborada para la recopilación de información (ver **ANEXO II**) a 300 personas del área administrativa y 300 personas del área académica (es decir el 9% de cada área).

Tras el envío del comunicado informativo, la DTI[9] se encargó de la digitalización de la encuesta y la DCI[10] efectuó el envío de las encuestas a la muestra seleccionada, brindando un plazo para su ejecución de catorce (14) días calendario.

Se obtuvieron los siguientes detalles luego de cumplido el plazo para la ejecución de la encuesta:

DETALLES DE LA MUESTRA TOTAL				
Área	Personal total	#de invitados	# de participantes	%
Académica	3321	300	47	16%
Administrativa	3366	300	50	17%

Tabla 10 - Muestra total de la encuesta realizada

En base a la muestra final (97 participantes en total), se obtuvo información importante para el diagnóstico del presente proyecto (ver **ANEXO III**).

[9] DTI: Dirección de Tecnologías de Información de la Universidad Católica
[10] DCI: Dirección de Comunicación Institucional de la Universidad Católica

ANEXO III
ENCUESTA DE DIAGNÓSTICO

ENCUESTA DE DIAGNOSTICO

"CONCIENTIZACION EN SEGURIDAD DE LA INFORMACION"

1. ¿Qué entiende por Seguridad de la Información?

2. Qué caracteristicas tiene para Ud. un virus informático:

		SI	NO
1	No es dañino		
2	Los virus solo atacan a personas que entran a páginas no deseadas		
3	Es nocivo, pero solo se previenen con el correcto uso de internet		
4	Es riesgoso, por lo cual es necesario tomar precauciones.		

3. ¿Qué entiende por incidente en Seguridad de la Información?

4. ¿Ud. ha sido victima de un incidente en Seguridad de la Información?

SI	NO

Especifique cuál: _____

5. Si Ud. es afectado por un incidente en Seguridad de la Información ¿A quién acudiría?

a) Dirección de Administración y Finanzas
b) Oficina de Contraloría
c) Sección de Seguridad de la Información
d) DIRINFO
e) Dirección de Recursos Humanos
f) G4S
g) Otra: _____.

6. ¿Por qué es importante reportar un incidente de Seguridad de la Información a la brevedad? *(opción múltiple)*

a) Para que solo obtenga una rápida atención
b) Para no tener responsabilidad frente al daño potencial
c) Para que se minimice el daño potencial.
d) Para dar mayor tiempo en la investigación y solución del incidente

7. ¿Quién es responsable de la Seguridad de la Información en la Universidad?

8. Tiene la Universidad una unidad o persona asignada para labores exclusivas de Seguridad de la Información.

SI	NO

¿Qué unidad o persona? : _____

9. ¿Qué tan valiosa considera Ud. que es la información contenida dentro de su computadora para ser sustraída y que impacte de manera negativa para la Universidad?

a) Muy valiosa
b) Valiosa
c) Considerablemente valiosa
d) Poco valiosa
e) No es valiosa

10. ¿Con que frecuencia realiza copias de respaldo a su información?

a) diaria
b) varias veces a la semana
c) Mensualmente
d) Otra frecuencia: _____
e) No realizo copias de respaldos de la información

11. ¿A través de qué dispositivos visualiza su cuenta de correo electrónico laboral de la PUCP? *(opción múltiple)*

a) Computadora de Trabajo
b) Computadora Personal
c) Tablet
d) Smartphone

12. ¿Mediante qué medios comparte información con sus compañeros de trabajo?

	ARCHIVO	SI	NO
1	Carpetas compartidas		
2	USB		
3	Correo electrónico		
4	Documentos en físico		
5	Otros (Especifique)		

13. ¿Un compañero de trabajo ha compartido su contraseña con Ud.?

SI	NO

Motivo: _____

14. ¿Algún compañero de trabajo ha tenido acceso a su computadora?

SI	NO

Motivo: _____

15. ¿Ha recibido capacitaciones o inducciones de Seguridad de la Información impartidas por la Universidad?

SI	NO

Especifique cuál: _____

16. ¿Qué canales de comunicación de la Universidad considera pertinente para la difusión en Seguridad de la Información? (Enumere la prioridad del 1 al 7, siendo 1 el más usado)

	Medio de comunicación	SI	NO	PRIORIDAD
1	Correo Electrónico			
2	Afiches			
3	Puntoedu impreso			
4	Puntoedu virtual			
5	Charlas informativas			
6	Revista PUCP			
7	Fanpage (Facebook)			

ANEXO IV
RESULTADOS DE LA ENCUESTA

Pregunta 1: ¿Qué entiende por Seguridad de la Información?

En general, los encuestados asocian la Seguridad de Información con el cuidado y resguardo de toda información tanto en dispositivos electrónicos como de documentos en físico. No obstante, algunas personas sólo consideran que la Seguridad de Información refiere a la información virtual o todo aquello relacionado a tecnología.

Un dato relevante en las respuestas analizadas es que para muchos usuarios la responsabilidad recae en las medidas que toma la Universidad respecto al tema, tales como la generación de políticas e incluso del respaldo de la información; más que en su propia responsabilidad. Para esta población, se requiere concientización del rol que ellos cumplen en Seguridad de la Información.

Dentro de los ejemplos de medidas de Seguridad de la Información, se recopiló lo siguiente:

- ✓ Cambiar periódicamente la contraseña de las cuentas de correo electrónico.
- ✓ Usar correctamente de los dispositivos electrónicos para menguar el ingreso de virus informáticos.
- ✓ Cuidar los documentos en físico mediante compartimientos con llave.
- ✓ Al momento de botar a la basura o al reciclar documentos que contengan información confidencial, estos deben ser destruidos acuciosamente.
- ✓ Evitar la exposición de información (virtual, documentos en físico, información verbal) a terceros que puedan interpretar o emplear la información de forma errónea.
- ✓ Conocer las medidas preventivas como Seguridad de la Información.
- ✓ Conocer las alternativas de reacción frente a incidentes en Seguridad de la Información.

Pregunta 2: ¿Qué características tiene para Ud. un virus informático?

ÁREA ADMINISTRATIVA						
RESPUESTA	SI		NO		EN BLANCO	
	Cantidad	%	Cantidad	%	Cantidad	%
Es dañino	45	90%	1	2%	4	8%
Los virus solo atacan a personas que entran a páginas no deseadas	6	12%	38	76%	6	12%
Es nocivo, pero solo se previene con el correcto uso de internet	23	46%	21	42%	6	12%
Es riesgoso, por lo cual es necesario tomar precauciones	49	98%	1	2%	0	0%

Muestra: 50

ÁREA ACADÉMICA						
RESPUESTA	SI		NO		EN BLANCO	
	Cantidad	%	Cantidad	%	Cantidad	%
Es dañino	45	96%	2	4%	0	0%
Los virus solo atacan a personas que entran a páginas no deseadas	6	13%	38	81%	3	6%
Es nocivo, pero solo se previene con el correcto uso de internet	17	36%	24	51%	6	13%
Es riesgoso, por lo cual es necesario tomar precauciones	46	98%	0	0%	1	2%

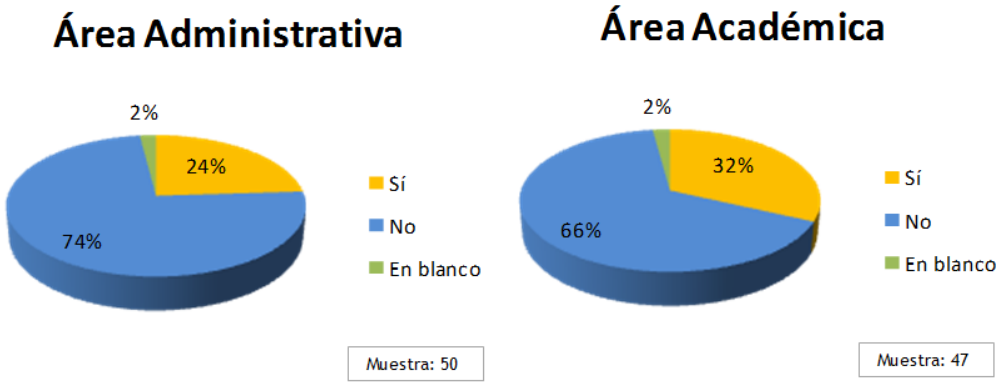
Muestra: 47

Pregunta 3: ¿Qué entiende por incidente en Seguridad de la Información?

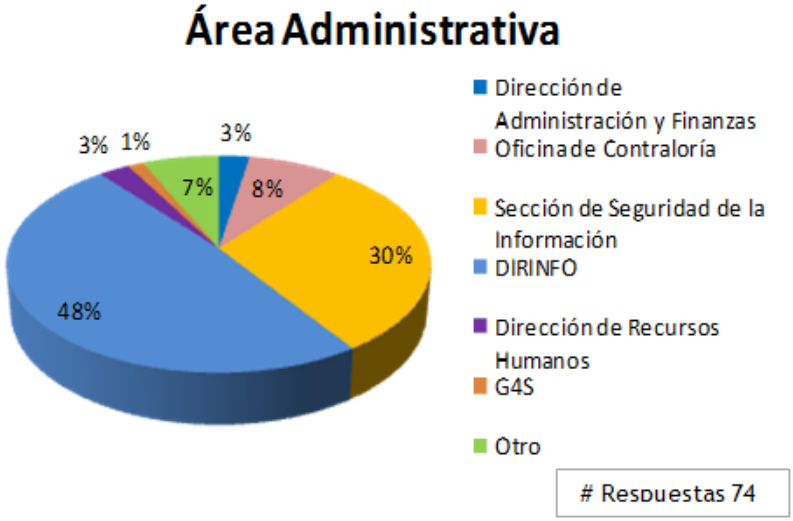
Las respuestas expuestas giran en torno a las siguientes afirmaciones:

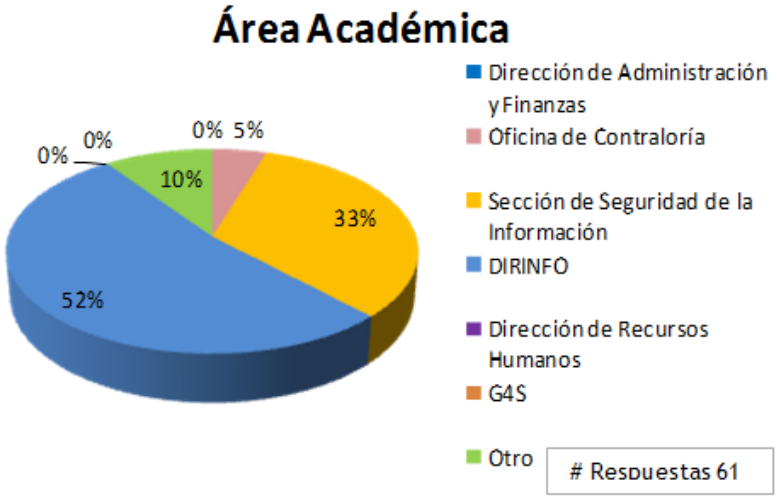
- ✓ Pérdida de información que no está resguardada y es irrecuperable.
- ✓ Acceso de personal externo a información de la PUCP.
- ✓ Intento de ingreso a información personal electrónica del usuario.
- ✓ Cualquier filtro de información confidencial (incluso verbal).
- ✓ Ingreso de un virus a la computadora.
- ✓ Ingreso al correo del usuario por parte de un tercero.
- ✓ Hackeo de la computadora laboral o personal (en el caso del área académica).

Pregunta 4: ¿Ud. ha sido víctima de un incidente en Seguridad de la Información?

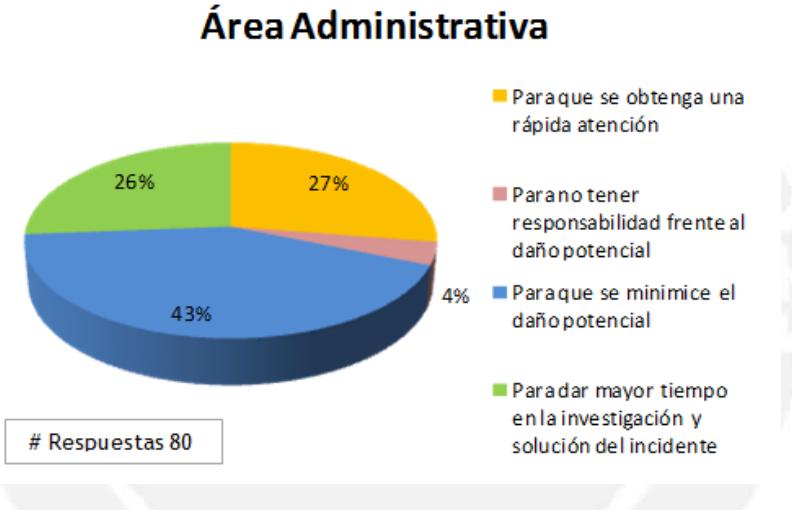


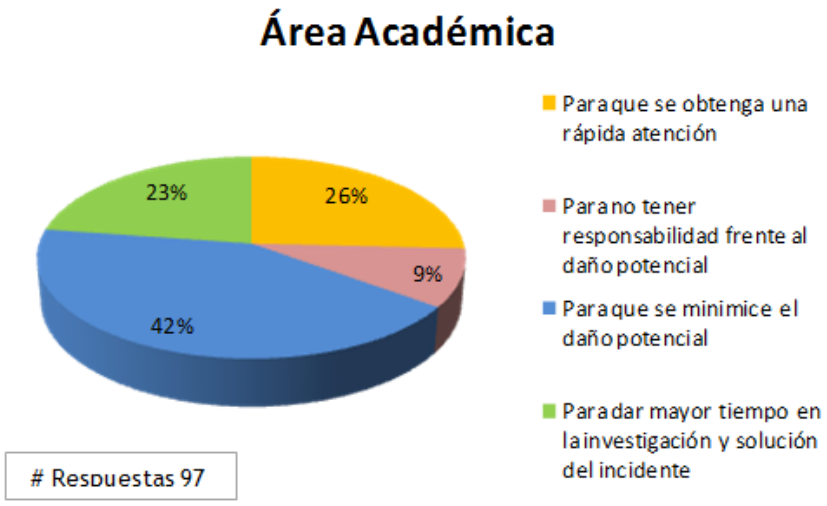
Pregunta 5: Si Ud. es afectado por un incidente en Seguridad de la Información ¿A quién acudiría?





Pregunta 6: ¿Por qué es importante reportar un incidente de Seguridad de la Información a la brevedad?



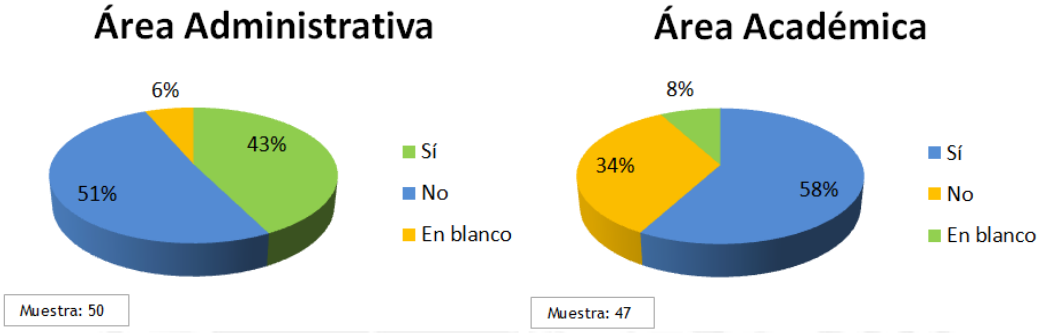


Pregunta 7: ¿Quién es responsable de la Seguridad de la Información en la Universidad?

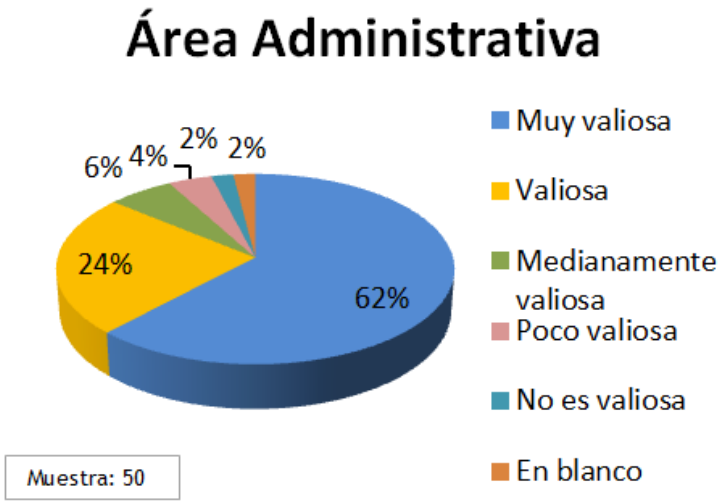
Aproximadamente un tercio de la muestra total sí considera que tienen un rol dentro de la Seguridad de la Información, en muchos de estos casos, comparten la responsabilidad con distintas entidades de la Universidad.

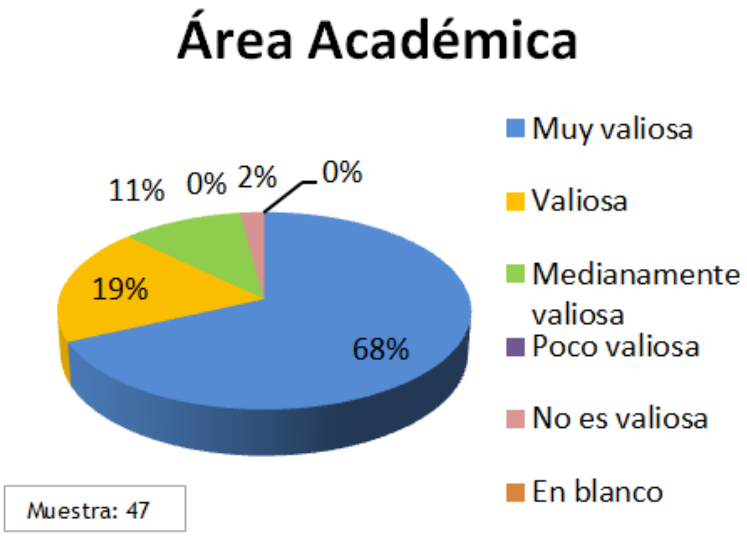
Ambas áreas identifican a DTI como el principal responsable de los temas relacionados a Seguridad de la Información.

Pregunta 8: Tiene la Universidad una unidad o persona asignada para labores exclusivas de Seguridad de la Información

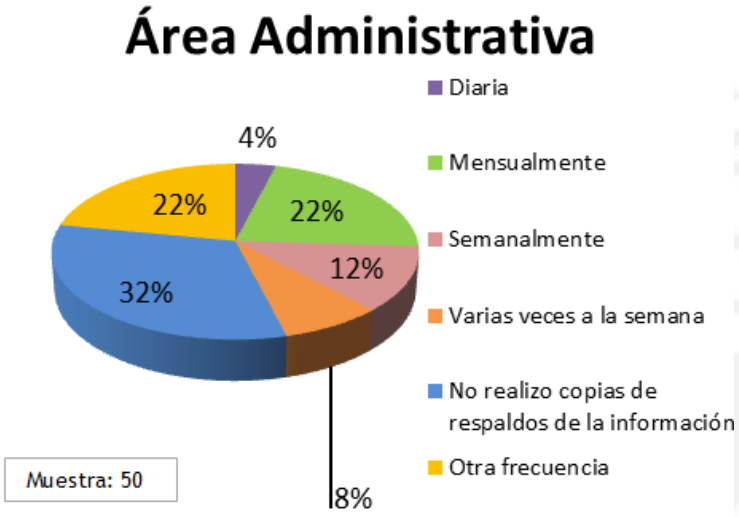


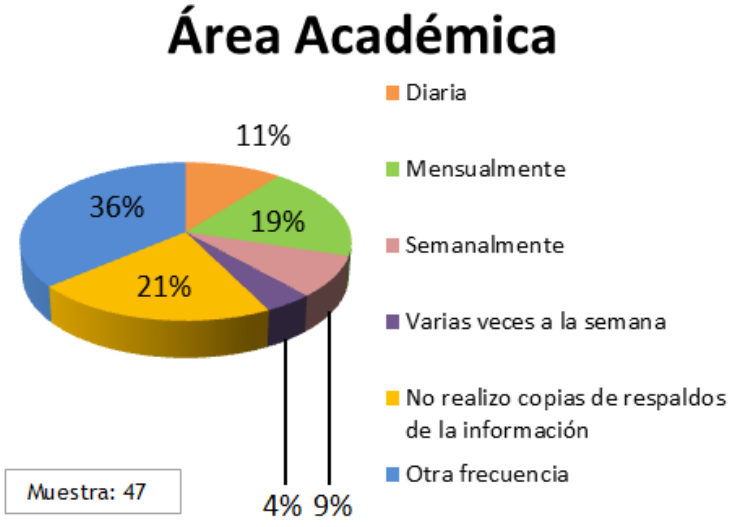
Pregunta 9: ¿Qué tan valiosa es, para Ud. y/o para la Universidad, la información que contiene en su computadora?



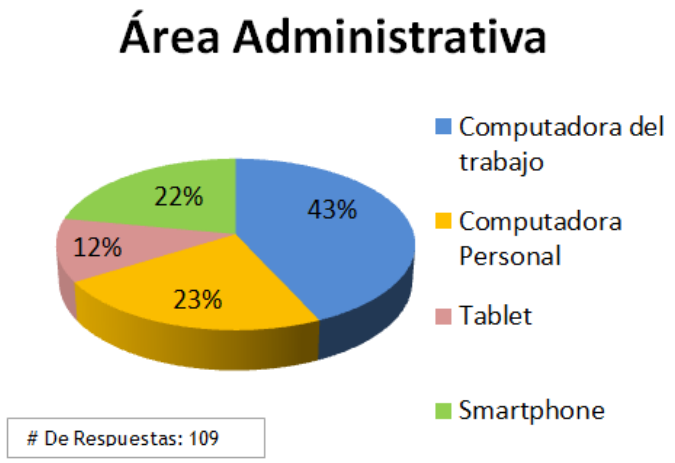


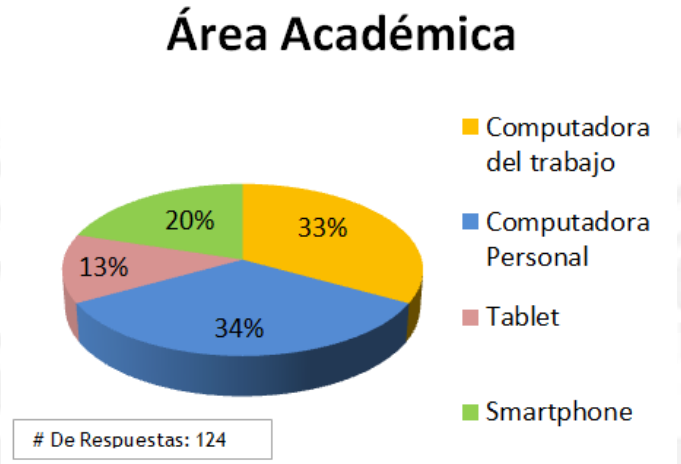
Pregunta 10: ¿Con qué frecuencia realiza copias de respaldo a su información?



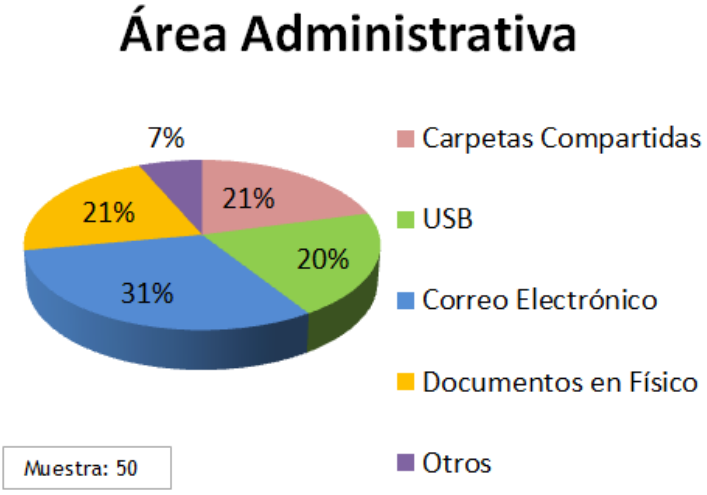


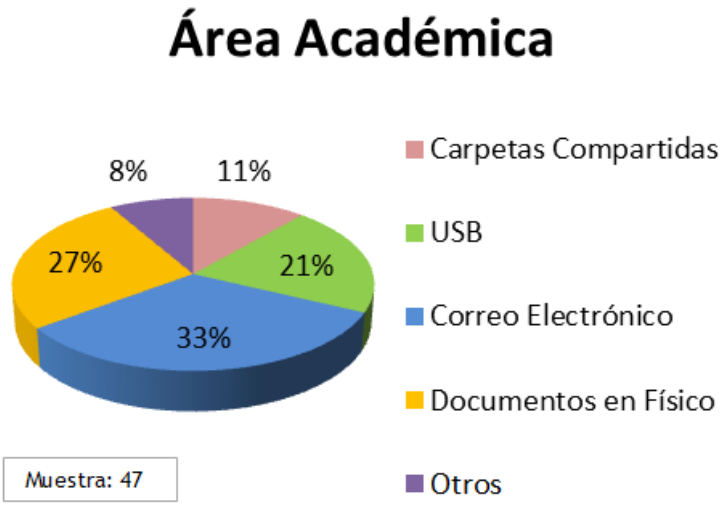
Pregunta 11: ¿A través de qué dispositivos visualiza su cuenta de correo electrónico laboral de la PUCP?



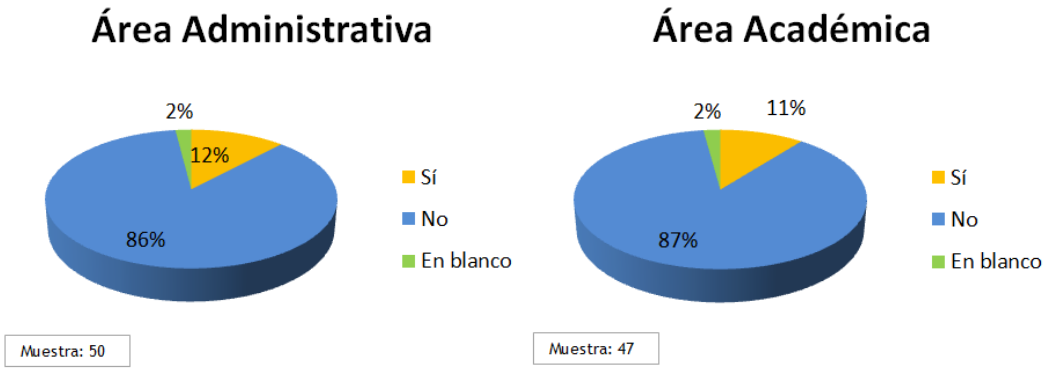


Pregunta 12: ¿Mediante qué medios comparte información con sus compañeros de trabajo?

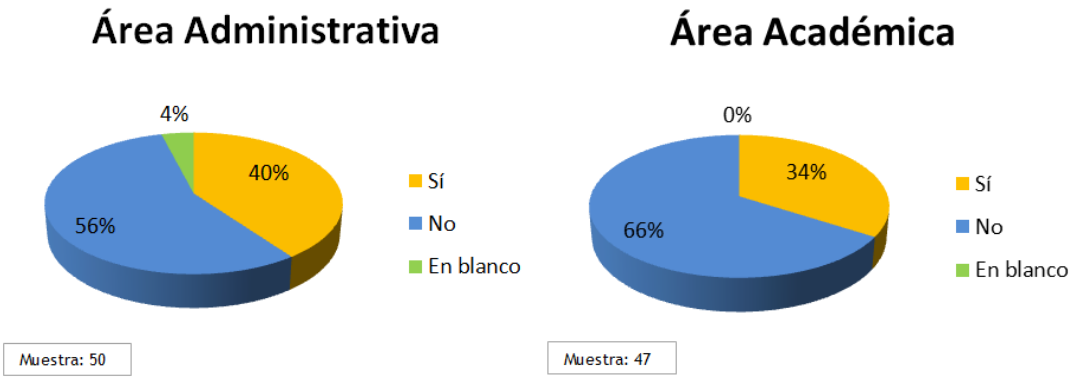




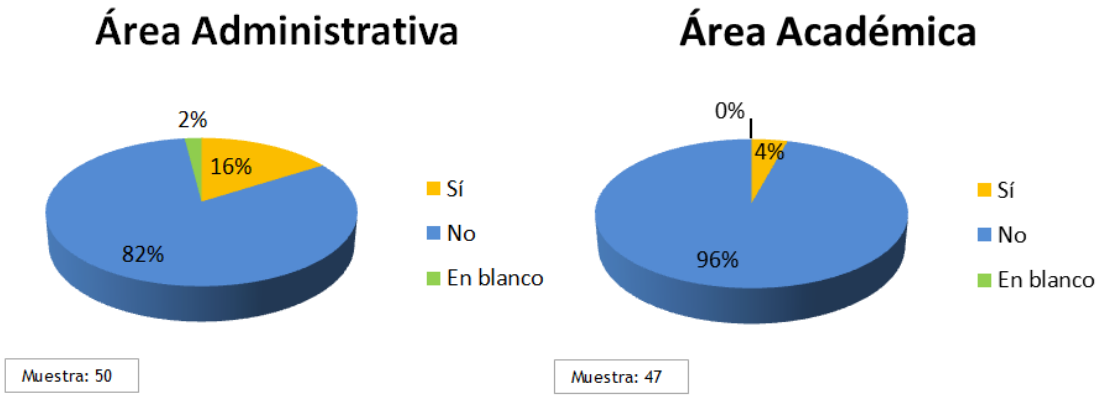
Pregunta 13: ¿Un compañero de trabajo ha compartido su contraseña con Ud.?



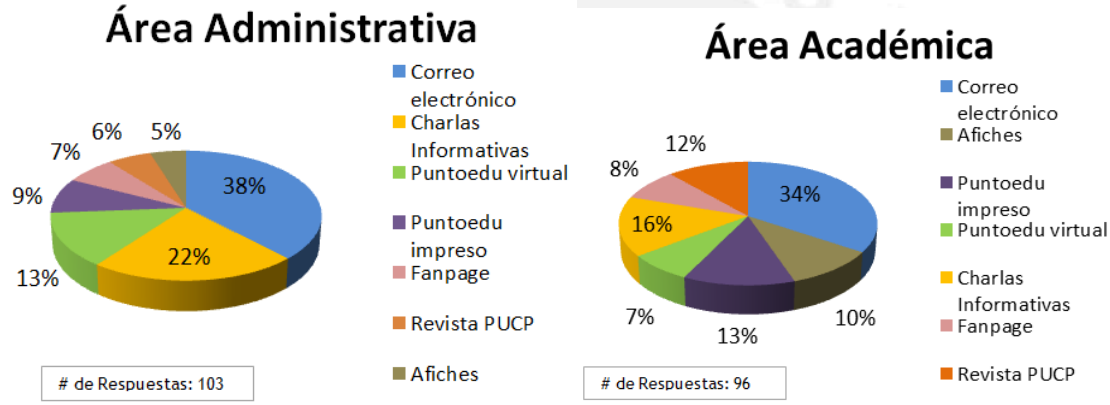
Pregunta 14: ¿Algún compañero de trabajo ha tenido acceso a su computadora?



Pregunta 15: ¿Ha recibido capacitaciones o inducciones de Seguridad de la Información impartidas por la Universidad?



Pregunta 16: ¿Qué canales de comunicación son pertinentes para la difusión en Seguridad de la Información? Enumere la prioridad del 7 al 0, siendo 7 el más usado y 0 el no pertinente



ANEXO V
PRE TEST

1. OBJETIVOS

1.1. Objetivo General

Lograr un entendimiento del personal administrativo con la finalidad de definir y/o rectificar las estrategias que permitan la adecuada ejecución del Plan de Comunicación en Seguridad de Información.

1.2. Objetivos Específicos

a) Conocer la disposición e interés del sector administrativo sobre la incorporación de buenas prácticas de la Seguridad de la Información.

b) Identificar el canal de comunicación y el contenido adecuado para la difusión de la Campaña de la Seguridad de Información.

c) Conocer sus apreciaciones y sugerencias respecto a la Campaña de Comunicación en la Seguridad de Información.

2. FICHA TÉCNICA

Naturaleza del Estudio: Estudio Cualitativo

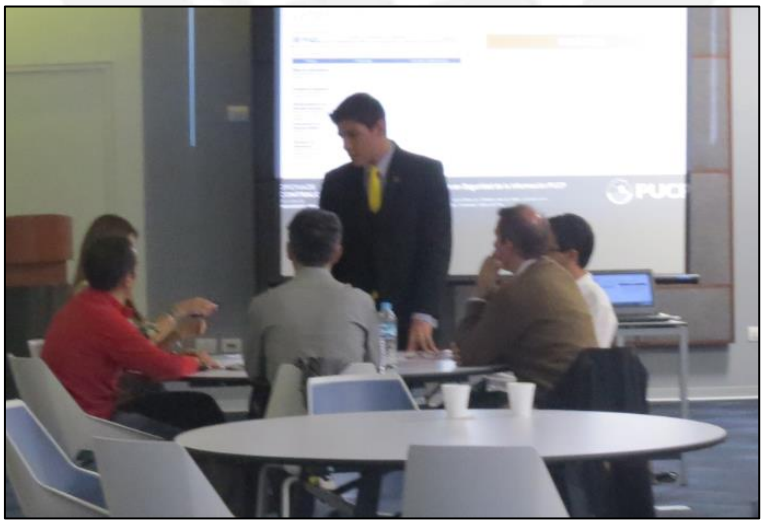
Público Objetivo: Administrativos, a tiempo parcial o tiempo completo, con más de un año de relación laboral con la Universidad PUCP que tienen actividades de docencia.

N° de Participantes: 5 administrativos

Fecha del Estudio: miércoles, 27 de junio de 2016

Lugar: Aula Polivalente – CIA PUCP

Duración: 60 minutos



ANEXO VI
ENTREVISTAS DE POTENCIAL DE INFLUENCIA

Nombre:	CPCC José Rincón Macote, ISO31000 RM, COBIT5 F	
Cargo:	Contralor General PUCP	
Notoriedad: ¿Cuán conocida cree que es el área de seguridad de la información?	6	9
Notabilidad: ¿Qué tanto valora el área de seguridad de la información?	6	9
Compromiso: ¿Qué tan comprometida cree que están las Altas Autoridades PUCP para desarrollar acciones de gestión de intereses?	6	8
Estratégico: ¿En qué posición de reporte se encuentra el área de Seguridad de la Información? (Estratégico u Operativo)	8	9
Sistemático: ¿Se encuentra esquematizado el proceso de seguridad de la información?	6	8
Proactivo: ¿El área de Seguridad de la Información tiene más un rol proactivo o reactivo?	3	9
	ACTUAL	**ESPERADO**

Nombre:	Mg. Luis Ángel Gutierrez Villavicencio, CISA, CISM, ISO31000 RM, ISO27001 LI	
Cargo:	Jefe de Seguridad de la Información PUCP	
Notoriedad: ¿Cuán conocida cree que es el área de seguridad de la información?	7	9
Notabilidad: ¿Qué tanto valora el área de seguridad de la información?	8	9
Compromiso: ¿Qué tan comprometida cree que están las Altas Autoridades PUCP para desarrollar acciones de gestión de intereses?	6	8
Estratégico ¿En qué posición de reporte se encuentra el área de Seguridad de la Información? (Estratégico u Operativo)	8	9
Sistemático ¿Se encuentra esquematizado el proceso de seguridad de la información?	6	8
Proactivo ¿El área de Seguridad de la Información tiene más un rol proactivo o reactivo?	3	9
	ACTUAL	**ESPERADO**