UNIVERSIDAD NACIONAL DE LOJA

Facultad de la Energía, las Industrias y los Recursos Naturales No Renovables

CARRERA DE INGENIERÍA EN SISTEMAS

Plan piloto para la mitigación de ciberataques bajo la modalidad de Ingeniería Social en la Universidad Nacional de Loja

Tesis de Grado previa a la obtención del título de Ingeniera en Sistemas.

Autor:

- Jessica Mariuxi Pineda Criollo.

Director:

- Ing. Valeria del Rosario Herrera Salazar

LOJA –ECUADOR

2020

CERTIFICACIÓN:

Ing. Valeria del Rosario Herrera Salazar, Mg. Sc.
DIRECTORA DE TESIS.

CERTIFICA:

Que la Srta. Egresada Jessica Mariuxi Pineda Criollo autora del presente Trabajo de Tesis denominada “PLAN PILOTO PARA LA MITIGACIÓN DE CIBERATAQUES BAJO LA MODALIDAD DE INGENIERÍA SOCIAL EN LA UNIVERSIDAD NACIONAL DE LOJA” ha sido dirigida, revisada y corregida bajo mi tutoría, cumpliendo los requisitos exigidos en una investigación de este nivel por lo cual autorizo su presentación y sustentación.

Loja, 28 de Febrero del 2020

Ing. Valeria Herrera
DIRECTORA DE TESIS

AUTORÍA:

Yo, Jessica Mariuxi Pineda Criollo, declaro ser la autora de la presente Tesis y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos y acciones legales, por el contenido de la misma.

Adicionalmente aceptamos y autorizamos a la Universidad Nacional de Loja la publicación de la tesis en el Repositorio Institucional.

Firma: 

Cedula: 1104959547.

Fecha: 28/07/2020

CARTA DE AUTORIZACIÓN DE TESIS POR PARTE DEL AUTOR, PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO.

Yo **JESSICA MARIUXI PINEDA CRIOLLO**, declaro ser la autora del trabajo de titulación: **PLAN PILOTO PARA LA MITIGACIÓN DE CIBERATAQUES BAJO LA MODALIDAD DE INGENIERÍA SOCIAL EN LA UNIVERSIDAD NACIONAL DE LOJA**, como requisito para optar al grado de: **INGENIERA EN SISTEMAS**; autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Digital Institucional:

Los usuarios pueden consultar el contenido de este trabajo en el RDI, en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad. La Universidad Nacional de Loja, no se responsabiliza por plagio o copia del trabajo de titulación que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los 28 días del mes de Julio del dos mil veinte.

Firma: 

Autora: Jessica Mariuxi Pineda Criollo

Cédula: 1104959547

Dirección: Loja (Ciudad Victoria, Tiradentes: Clotario Maldonado Paz y Jaime Hurtado)

Correo Electrónico: jmpinedac@unl.edu.ec

Celular: 0994833352

DATOS COMPLEMENTARIOS

Director de Trabajo de Titulación: Ing. Valeria del Rosario Herrera Salazar, Mg. Sc.

Tribunal de Grado: Ing. Hernán Leonardo Torres Carrión. Mg. Sc.
Ing. Mario Enrique Cueva Hurtado. Mg. Sc.
Ing. Cristian Ramiro Narváez Guillen. Mg. Sc.

AGRADECIMIENTO

Agradezco en primer lugar a Dios, quien con su bendición, apoyo y fortaleza ha permitido que cumpla cada meta propuesta.

A mis padres José Pineda y Marina Criollo quienes con su amor, paciencia y esfuerzo me han permitido llegar a cumplir hoy un sueño más, gracias por inculcar en mí el ejemplo de esfuerzo, responsabilidad y valentía.

A mis hermanas, cuñado, sobrinos, demás familiares y amigos, quienes, con su apoyo incondicional, consejos y palabras de aliento hicieron de mí una mejor persona y de una u otra forma me acompañan en todos mis sueños y metas.

Mi profundo agradecimiento a todas las personas que hacen la Unidad de Telecomunicaciones e Información UTI, por abrirme las puertas y permitirme desarrollar el presente Trabajo de Titulación.

Finalmente quiero expresar mi más grande y sincero agradecimiento a la Ing. Valeria Herrera y al Ing. Juan Carlos Riofrío principales colaboradores durante todo este proceso, quienes con su dirección, conocimiento, enseñanza y colaboración permitieron el desarrollo de este trabajo.

Jessica Pineda.

DEDICATORIA

A mi padre, José.

A mi madre, Marina.

A mi hermana, Diana.

A mi cuñado, Miguel.

A mi tío, Luis.

A mi tía, Esperanza.

Jessica Pineda.

TABLA DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. TÍTULO

Plan piloto para la mitigación de ciberataques bajo la modalidad de Ingeniería Social en la Universidad Nacional de Loja.

2. RESUMEN

Considerando que el ser humano es vulnerable a diferentes tipos de ciberataques como la Ingeniería Social, este se ha convertido en la principal causa de vulnerabilidades para la seguridad de la información. El presente trabajo de titulación tiene como propósito crear un plan piloto para la mitigación de ciberataques bajo la modalidad de Ingeniería Social en la Universidad Nacional de Loja, el cual se cumplió en cuatro fases. En la primera fase se desarrolló una Revisión Sistemática de Literatura SRL usando la metodología de Barbara Kitchenham y Brereton, la misma que permitió identificar 13 técnicas de ataque, y 11 salvaguardas para mitigar ciberataques bajo la modalidad de Ingeniería Social.

Durante la segunda fase se empleó la metodología de Margerit para realizar el Análisis de Riesgo, el mismo que dio a conocer que de las amenazas identificadas, 12 son consideradas como principales riesgos (nivel de riesgo: moderado, alto, y critico) a los que podría estar expuesto el usuario; además mediante la aplicación de la encuesta se conoció que los usuarios hacen uso inadecuado del internet en sus horas laborales y que desconocen del peligro a ser víctimas de un ataque de Ingeniería Social. Para la simulación del ciberataque se ejecutó la técnica del phishing utilizando el kit de herramientas de Ingeniería Social de Kali Linux, obteniendo resultados favorables para la sustentación del presente Trabajo de Titulación.

En la tercera fase mediante la estructura propuesta por la tesista se desarrolló el plan piloto que mitigará los ciberataques bajo la modalidad de Ingeniería Social. Y finalmente, en la cuarta fase se elaboró el documento formal del Plan Piloto y el material de capacitación y concientización para su socialización y entrega final.

SUMMARY

Considering that the human being is vulnerable to different types of cyber attacks such as Social Engineering, this has become the main cause of vulnerabilities for information security. The purpose of the present degree work is to create a pilot plan for the mitigation of cyberattacks under the modality of Social Engineering at the National University of Loja, which was accomplished in four phases. In the first phase a Systematic Review of Literature SRL was developed using the methodology of Barbara Kitchenham and Brereton, which allowed the identification of 13 attack techniques, and 11 safeguards to mitigate cyber attacks under the modality of Social Engineering.

During the second phase, the Margerit methodology was used to carry out the Risk Analysis, which revealed that of the threats identified, 12 are considered to be the main risks (risk level: moderate, high and critical) to which the user could be exposed. For the simulation of the cyber attack, the phishing technique was executed using the Kali Linux Social Engineering toolkit, obtaining favourable results for the support of the present Degree Project.

In the third phase, through the structure proposed by the thesis student, a pilot plan was developed that will mitigate cyber-attacks under the Social Engineering modality. And finally, in the fourth phase, the formal document of the Pilot Plan and the training and awareness material for its socialization and final delivery were developed.

3. INTRODUCCIÓN

En la actualidad uno de los activos más valiosos para cualquier organización pública o privada es la información; a pesar que los especialistas en la seguridad de la información de cada empresa han implementado estrategias, soluciones y herramientas de protección, no han logrado mitigar de manera efectiva los múltiples tipos de ataques existentes en la actualidad, esto debido a que no se han preocupado por implementar mecanismos de seguridad en relación al usuario, convirtiéndolo así en el eslabón más débil de una organización, el mismo que es susceptible a ataques de ingeniería social [1].

La ingeniería social es una modalidad de ataque informático para obtener acceso a edificios, sistemas o datos (información susceptible) mediante la explotación de la psicología humana [2][3][4].

En base a lo antes mencionado se desarrolló el presente Trabajo de Titulación que tiene como objetivo principal "Crear el plan piloto para la mitigación de ciberataques bajo la modalidad de Ingeniería Social en la Universidad Nacional de Loja". Para dar cumplimiento al objetivo principal se plantearon cuatro objetivos específicos: 1) Revisión bibliográfica entorno a la ingeniería social; 2) Simular un ciberataque bajo la modalidad de Ingeniería Social; 3) Desarrollar el plan piloto para mitigar los ciberataques bajo la modalidad de ingeniería social; 4) Documentar el plan piloto y elaborar el material necesario de concientización para mitigar los ciberataques bajo la modalidad de ingeniería social.

El presente trabajo de titulación consta de varias secciones, que son:

Revisión de literatura	En esta sección se abordaron los siguientes temas: ingeniería social, técnicas de ciberataque bajo la modalidad de Ingeniaría Social, usuario, atacante de ingeniería social, ciberataque o ataque informático, delito informático, seguridad de la Información, controles y contramedidas, estándar ISO/IEC 27002:2013. Además, se abordó el marco legal en cual se sustenta este TT.

Trabajos relacionados	En esta sección se hace referencia a trabajos similares que aportaron favorablemente al presente trabajo.
Materiales y métodos	En esta sección se describen los métodos (M. Inductivo, M. de Revisión Sistemática de Literatura, M. de Enmascaramiento), metodologías (M. de Bárbara Kitchenham y Brereton, M. Margerit v3, M. para la simulación del ciberataque), técnicas (Encuesta, Simulación, Muestreo Aleatorio Simple) y los materiales (Software, hardware, y materiales varios) usados para la realización del presente trabajo.
Resultados	En esta sección se presenta los resultados obtenidos al dar cumplimiento a cada uno de los objetivos planteados para este Trabajo de Titulación.
Discusión	Se describe el proceso realizado para cumplir los objetivos planteados y se realiza la interpretación de los resultados obtenidos.
Conclusiones	Se destacan los resultados más importantes del cumplimiento de los objetivos planteados.
Recomendaciones	Se presentan sugerencias para mejorar los resultados del presente TT.

4. REVISIÓN DE LITERATURA

En esta sección se describen los conceptos para tener una mejor comprensión del tema y la base legal que sustenta el presente TT.

4.1. Conceptos Preliminares

4.1.1. Ingeniería Social

La ingeniería social es la combinación de técnicas basadas en humanos o en tecnología, las cuales son utilizadas por atacantes maliciosos para explotar al eslabón más débil de una organización, con el fin de obtener información confidencial o realizar acciones para comprometer la seguridad de la información [5][6][7][8].

4.1.2. Técnicas de ciberataque bajo la modalidad de Ingeniaría Social.

Entre las técnicas de ciberataque que pretenden persuadir al ser humano para que el ingeniero social acceda a la información confidencial, tenemos las siguientes:

- **T01) Phishing:** Busca engañar al usuario a través del envío de correos electrónicos fraudulentos, con el objetivo de influir u obtener información personal [6][9][10].
- **T02) Baiting:** El atacante deja un dispositivo infectado, como una unidad USB, un teléfono celular o una tarjeta de memoria en algún lugar a propósito, donde personas escogidas específicamente puedan encontrarlo e infectar sus computadores [6][11][12].
- **T03) Smishing:** El atacante usa mensajes de teléfono móvil (SMS) para lograr que las víctimas tomen acciones inmediatas con el objetivo de influir u obtener información personal [13][14].
- **T04) Quid Pro Quo:** El atacante promete algún beneficio a la víctima a cambio de información sensible de la organización o del mismo usuario [6][10].
- **T05) Pretexting:** El atacante crea un escenario inventado para engañar al usuario, con el objetivo de robar información importante y sensible a la víctima [6][15].
- **T06) Pharming:** El atacante se infiltra en un sistema informático e instala un código malicioso que hace que el tráfico del sitio web del sistema se redirija a sitios falsos desarrollados por el pirata informático [16][17][18].

- **T07) Vishing:** El atacante realiza llamadas telefónicas suplantando a compañías de servicios o de gobierno mediante las cuales se busca engañar a la víctima para que revele información privada [6][9][19].
- **T08) Spear - phishing:** El atacante utiliza el correo electrónico o comunicaciones electrónicas para engañar a personas concretas u organizaciones específicas [20][21][22] **.**
- **T09) Dumpster Diving:** El atacante busca en la basura documentos y otros materiales para obtener información útil sobre una organización, empresa, o individuo [15][23].
- **T10) Shoulder Surfing:** El atacante recopila información personal o privada a través de la observación directa en una pantalla por estar físicamente cerca de ella y tener acceso a la lectura de la información digitada por la víctima [15][23][2].
- **T11) Espionaje Industrial:** El atacante consigue introducirse en los sistemas informáticos de la empresa y robar información valiosa para obtener una ventaja comercial [15][24][25].
- **T12) Taigating:** El atacante obtiene el acceso a las áreas restringidas como oficinas o centros de datos, mediante el engaño o descuido de una persona con la autorización correspondiente [11][26][27].
- **T13) Scareware:** Es una táctica de malware que manipula a los usuarios para que descarguen, instalen o compren software malintencionado que exponga datos confidenciales [1][28][29].

4.1.3. Usuario

Los usuarios son aquellas personas que cumplen un rol dentro de la institución, y que son responsables por el uso de la información que manejan dentro de la misma.

4.1.4. Atacante de Ingeniería Social

Un atacante de Ingeniería Social es la persona que intenta crear un estado de confianza con la víctima, facilitando la recogida de información o haciendo que la víctima ejecute alguna acción involuntaria que comprometa la seguridad de la información [9][15][30].

4.1.5. Ciberataque o Ataque Informático

Un ciberataque consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, hardware, e incluso, en las personas que forman parte de un ambiente informático; con el objetivo de comprometer la confidencialidad, disponibilidad o integridad del equipo, red o sitio web atacado y de la información contenida o transmitida a través de ellos [31].

4.1.6. Delito Informático

Un delito informático es toda acción no ética, o no autorizada, en las que se tienen a las computadoras como instrumento o fin, provocando un perjuicio a personas o entidades [32][33][34].

4.1.7. Seguridad de la Información.

La Seguridad de la Información son medidas de protección enfocadas a preservar la confidencialidad, integridad y disponibilidad de la información [35][36].

- **Confidencialidad:** Es la necesidad de que la información solo sea conocida por personas autorizadas [35][36][37].
- **Integridad:** Es la característica que hace que el contenido de la información permanezca inalterado, a menos que sea modificado por personal autorizado [35][36][37].
- **Disponibilidad:** Es la capacidad que tiene la información para permanecer accesible, en el momento y en la forma en que los usuarios que estén autorizados lo requieran [35][36][37].

4.1.8. Controles y Contramedidas (Salvaguardias)

- **Controles:** Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal [36].
- **Contramedidas:** Son aquellos procedimientos o mecanismos utilizados para protegerse de una amenaza de Ingeniería Social [36].

4.1.9. Estándar ISO/IEC 27002:2013

Esta norma es una guía de buenas prácticas a través de las cuales una institución o empresa puede mejorar la seguridad de la información [37][38].

La siguiente figura muestra la estructura de la ISO/IEC 27002:2013:

***FIGURA1**: Estructura de la ISO/IEC 27002:2013*

La norma contiene 14 dominios de control de seguridad, 35 objetivos de control y 114 controles.

En base a la estructura presentada de la ISO/IEC 27002:2013, se han considerado los siguientes dominios de control de seguridad para el presente trabajo de TT:

***FIGURA 2:** Dominios de control de seguridad considerados en el presente TT.*

4.1.10. Marco legal

El marco legal proporciona los documentos oficiales para prevenir o penalizar tanto a la institución como al usuario de las acciones relacionadas al manejo adecuado de la información, entre estos documentos se hace referencia a:

4.1.10.1. Ley del Sistema Nacional de Registro de Datos Púbicos

En su capítulo 2, respecto a los PRINCIPIOS GENERALES DEL REGISTRO DE DATOS PUBLICOS específicamente en el Art. 4.- Responsabilidad de la información establece lo siguiente [39]:

"(..) ***Art. 4.- Responsabilidad de la información. -*** *Las instituciones del sector público y privado (…), son responsables de la integridad, protección y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros (…)"*

4.1.10.2. Esquema Gubernamental de Seguridad de da Información EGSI

En su sección 4, respecto a la SEGURIDAD DE LOS RECURSOS HUMANOS específicamente en los puntos 4.4. Responsabilidades de la dirección a cargo del funcionario, 4.5. Educación, formación y sensibilización en seguridad de la información establece lo siguiente:

"(...) ***4.4. Responsabilidades de la dirección a cargo del funcionario.*** *(...) b) Lograr la concienciación sobre la seguridad de la información correspondiente a sus funciones y responsabilidades dentro de la institución. c) Acordar los términos y las condiciones laborales, las cuales incluyen la política de la seguridad de la información de la institución y los métodos apropiados de trabajo. (...) "*

"(...) ***4.5. Educación, formación y sensibilización en seguridad de la información.*** *a) Socializar y capacitar de forma periódica y oportuna sobre las normas y los procedimientos para la seguridad, las responsabilidades legales y los controles de la institución, así como en la capacitación del uso correcto de los servicios de información. "*

4.1.10.3. Políticas de Telecomunicaciones, Desarrollo de Software, Redes de La Universidad Nacional de Loja.

Sección 1, respecto a las POLÍTICAS UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN específicamente en las Políticas de Administración de Recursos, Políticas de Salvaguarda y Confidencialidad, Políticas de protección de datos y sistemas establecen lo siguiente:

"(…) ***1.2. Políticas de administración de recursos.*** *(...) La UTI deberá proveer los mecanismos de protección y controles necesarios que aseguren la integridad y privacidad de los datos almacenados en los archivos y bases de datos que tenga en custodia (…)".*

"(...) ***1.5. Políticas de Salvaguarda y Confidencialidad.*** *Los funcionarios de la UTI bajo cualquier forma de estructura, se comprometen a salvaguardar de todo riesgo y a guardar la más absoluta reserva y/o confidencialidad sobre toda la información, cualquiera sea su naturaleza (...) "*

"1.6. Políticas de Protección de datos y sistemas. (...) queda prohibido al usuario realizar intervenciones no debidas, entre las que se encuentran:

- *Manipulación no autorizada.*
- *Apertura, reemplazo y/o desconexión de componentes.*
- *Reasignaciones permanentes o temporales sin autorización.*
- *Instalación de programas, sistemas, módulos y/o archivos externos.*
- *Empleo de juegos y/o programas con fines no laborales.*
- *Modifica la configuración de sistemas, programas o dispositivos.*
- *Desinstalar sistemas, programas, módulos oficiales de la Universidad Nacional de Loja.*
- *Conexión a redes eléctricas o de Datos no certificadas y o autorizadas (...)"*

Sección 5, respecto a las **POLÍTICAS DE LA SECCIÓN DE REDES Y EQUIPOS INFORMÁTICOS** específicamente en las Políticas de uso de red, y Obligaciones del Usuario establecen lo siguiente:

"(...) ***5.4. Políticas de uso de red.*** *(...) Es responsable el usuario por los sitios que visite en internet; El usuario es responsable de la información (audio, video, documentos, etc.) que baje de Internet o Intranet (...); (...) Los usuarios gozan de*

privacidad de su información, con la excepción de aquellos en los que se detecten acciones que pongan en riesgo la seguridad de la red del campus universitario. (...)"

"(...) ***5.6. Obligaciones del Usuario.*** *(...) El alumno, docente o empleado es completamente responsable de todas las actividades realizadas con su cuenta de correo proporcionada por la UTI.*
(...)(...) El buen uso de su cuenta se entiende por:

- *Usar su cuenta con fines académicos y/o investigación.*
- *Respetar las cuentas de otros usuarios.*
- *No mandar ni contestar cadenas de correo.*
- *No usar su cuenta para fines comerciales.*
- *No enviar material obsceno o con intención de intimidar, insultar o acosar (...)"*

4.1.10.4. Ley penal ecuatoriana - Código Orgánico Integral Penal COIP

Dado que la Ingeniería Social es una modalidad de ataque para explotar vulnerabilidades humanas que permitan obtener información de un usuario o institución de manera ilegítima, lo cual conlleva a que se materialice un delito, el mismo que puede ser tipificado por el Código Orgánico Penal Integral COIP (ver ANEXO 1, sección "a"), en sus artículos:

TABLA 1: *Código Orgánico Integral Penal COIP - Artículos que penalizan un ataque de Ingeniería Social*

CÓDIGO ORGÁNICO INTEGRAL PENAL – COIP			TÈCNICAS DE INGENIERÌA SOCIAL QUE PENALIZA EL COIP												
ARTÍCULO	**DESCRIPCIÓN**	**PENA PRIVATIVA**	**T 01**	**T 02**	**T 03**	**T 04**	**T 05**	**T 06**	**T 07**	**T 08**	**T 09**	**T 10**	**T 11**	**T 12**	**T 13**
Artículo 178	Violación a la intimidad	1 a 3 años	X	X	X	X	X	X	X	X	X	X	X	X	X
Artículo 179	Revelación de secreto	6 meses a 1 año	X		X	X	X		X	X	X	X	X		
Artículo 180	Difusión de información de circulación restringida	1 a 3 años	X		X	X	X		X	X					
Artículo 181	Violación de propiedad privada	6 meses a 1 año												X	
Artículo 186	Estafa	5 a 7 años	X		X	X	X		X	X		X		X	X
Artículo 190	Apropiación fraudulenta por medios electrónicos	1 a 3 años	X		X	X	X	X	X	X		X	X	X	X
Artículo 212	Suplantación de identidad	1 a 3 años	X		X	X	X		X	X					
Artículo 229	Revelación ilegal de base de datos.	1 a 3 años						X				X	X		X
Artículo 230	Interceptación ilegal de datos	3 a 5 años	X	X	X	X		X	X	X	X	X	X	X	X

TABLA 1: *Código Orgánico Integral Penal COIP - Artículos que penalizan el uso ilegitimo de la información.*

CÓDIGO ORGÁNICO INTEGRAL PENAL – COIP			TÈCNICAS DE INGENIERÌA SOCIAL QUE PENALIZA EL COIP												
ARTÍCULO	**DESCRIPCIÓN**	**PENA PRIVATIVA**	**T 01**	**T 02**	**T 03**	**T 04**	**T 05**	**T 06**	**T 07**	**T 08**	**T 09**	**T 10**	**T 11**	**T 12**	**T 13**
Artículo 231	Transferencia electrónica de activo patrimonial	3 a 5 años	X	X	X	X	X	X					X		X
Artículo 232	Ataque a la integridad de sistemas informáticos	3 a 5 años	X	X				X		X			X	X	X
Artículo 234	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	3 a 5 años	X	X				X		X			X		
Artículo 235	Engaño al comprador respecto a la identidad o calidad de las cosas o servicios vendidos	6 meses a 1 año	X		X	X			X	X					X
Artículo 351	Infiltración en zonas de seguridad	6 meses a 2 años												X	

El análisis realizado a los 14 artículos del Código Orgánico Integral Penal COIP que podrían penalizar un delito de Ingeniería Social a sido corroborado por la opinión de una profesional entendida en derecho (ver ANEXO 1, sección “b”).

4.2. Trabajos Relacionados.

Los trabajos relacionados al desarrollo del presente trabajo de titulación TT[1], se detallan en base a los resultados presentados en la TABLA 2 de la Revisión Sistemática de Literatura SRL[2] realizada.

TABLA 2: *Trabajos relacionados entorno a la Ingeniería Social*

COD	DESCRIPCIÓN
AR02	En este trabajo desarrolla un modelo de ingeniería social que proporcione una mejor comprensión del proceso de ataque; para lo cual han utilizado dos escenarios de ataque, y a su vez han analizado los pasos del proceso de un ataque de ingeniería social con el fin de aplicar contramedidas mejoradas y oportunas tanto en una etapa temprana como en todas las etapas posteriores del proceso de ataque [7].
AR03	En este trabajo se presenta el caso de una prueba de penetración que utiliza técnicas de ingeniería social dirigidas a una gran empresa de telecomunicación en Croacia. Se describe el proceso de preparación, las técnicas utilizadas para las pruebas, los resultados y las lecciones aprendidas [9].
AR04	En este trabajo se determina el nivel de susceptibilidad de los usuarios a los ataques de ingeniería social en una organización, para lo cual se diseñaron dos escenarios de ataque, una campaña de phishing y un vector de intrusión física dirigidos a la población de usuarios de la organización (empleados) en base a la información disponible en Internet [20].
AR06	En este trabajo se describen las técnicas y estadísticas de ataques bajo la modalidad de Ingeniería Social. Así mismo se presenta un escenario típico de ataque de Phishing, en donde el atacante generará un correo electrónico el cual será enviado en nombre del equipo de soporte técnico de Gmail [6].
AR22	En este trabajo se presentan los marcos de ataque y los motivos de la propagación de los ataques de ingeniería social, y al final se proponen enfoques de defensa [40].
AR23	En este trabajo se analiza la historia de los ataques de phishing y la motivación de los mismos. También proporciona una taxonomía de los diversos tipos de ataques de phishing y de varias soluciones propuestas para proteger a los usuarios de este tipo de ataque [41].

[1] TT: Trabajo de Titulación
[2] SRL: Systematic Review of Literature (Revisión Sistemática de Literatura)

5. Materiales y Métodos

En esta sección se describen los materiales, herramientas, métodos, metodologías, y técnicas de investigación empleadas en el desarrollo y cumplimiento del presente TT.

5.1. Materiales.

Los recursos de hardware y software utilizados durante el desarrollo del TT son: la portátil que permitió cumplir con cada fase del proyecto; la impresora que se la utilizó para la impresión de documentos referentes al proyecto de titulación como avances y encuestas; Google Drive para almacenar la copia de seguridad de los avances del trabajo de titulación; Mendeley Desktop para realizar la gestión bibliográfica (Para citar o referenciar desde el procesador de texto); el procesador de texto para la creación, edición y modificación del documento de trabajo de titulación; Social Engineering toolkit para realizar la simulación del ciberataque de Ingeniería Social; Google Analytics para obtener el informe de los resultados de la simulación del ciberataque de Ingeniería Social; LucidChart para crear el material de capacitación y concientización; y Parsifal herramienta de apoyo que permitió realizar la revisión sistemática de la literatura.

5.2. Métodos.

5.2.1. Método Inductivo

Este método permitió comprender el trabajo realizado en cada artículo revisado para la SRL, identificando así el aporte de cada uno de éstos al presente TT.

5.2.2. Método de Revisión Sistemática de Literatura

Método para la revisión, selección y extracción de información, basado en la metodología de Bárbara Kitchenham y Brereton; el mismo que permitió afianzar los conocimientos acerca del tema del trabajo de titulación, y a desarrollar la revisión de literatura.

5.2.3. Método de Enmascaramiento.

Método usado para proteger la identidad del grupo de usuarios que conformaron la muestra poblacional, con el fin de evitar cualquier uso accidental o malintencionado posterior.

5.3. Técnicas.

5.3.1. Encuesta

Esta técnica se aplicó a un grupo de usuarios de la comunidad universitaria para recolectar información sobre la realidad que vive la institución acerca del uso del correo electrónico institucional, la creación de contraseñas, y en relación al tema a desarrollar.

5.3.2. Simulación

Esta técnica permitió simular un escenario para la ejecución de una de las amenazas bajo la modalidad de Ingeniería Social a la que se encuentra expuesta la comunidad universitaria, permitiendo al usuario interactuar de manera real con la amenaza ejecutada.

5.3.3. Muestreo Aleatorio Simple

Esta técnica permitió delimitar la muestra poblacional, en la cual todos los individuos de la población escogida tuvieron la misma posibilidad de participar en el desarrollo del presente trabajo.

La fórmula utilizada para delimitar la muestra poblacional fue la siguiente:

$$n = (Z^2pqN)/(Ne^2 + Z^2pq)$$

Donde:

N: población: Es el total de individuos que tienen ciertas características similares y sobre las cuales se desea hacer inferencia.

n: muestra: Es la parte de la población que se selecciona, de la cual se obtiene la información para el desarrollo del estudio. Es decir, representa el número de personas a las cuales se aplica la encuesta.

z: nivel de confianza: mide la confiabilidad de los resultados. Lo usual es utilizar un nivel de confianza de 95% (1.96) o de 90% (1.65). Mientras mayor sea el nivel de confianza.

e: grado de error: mide el porcentaje de error que puede haber en los resultados. Lo usual es utilizar un grado de error de 5% o de 10%. Mientras menor margen de error, mayor validez tendrán los resultados.
p: probabilidad de ocurrencia: Es la probabilidad de que ocurra un evento. Lo usual es utilizar una probabilidad de ocurrencia del 50%.
q: probabilidad de no ocurrencia: Es la probabilidad de que no ocurra un evento. Lo usual es utilizar una probabilidad de no ocurrencia del 50%. La suma de “p” más “q” siempre debe dar el 100%.

5.4. Metodologías.

5.4.1. Metodología de Bárbara Kitchenham y Brereton

Es la metodología empleada para realizar la revisión sistemática de literatura SRL, la cual cumple con el siguiente esquema:

a) Preguntas de investigación.
b) Proceso de búsqueda.
c) Definición de los criterios de inclusión y exclusión.
d) Definición de las bases de datos.
e) Cadenas de Búsqueda.
f) Evaluación de calidad.
g) Resultados

5.4.2. Metodología Margerit v3.

Margerit es una metodología para realizar el análisis de riesgos, ejecutando los siguientes pasos:

1) Determinar los activos relevantes para la Organización.
2) Determinar a qué amenazas están expuestos aquellos activos.
3) Determinar qué salvaguardas hay dispuestas.
4) Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza (probabilidad de ocurrencia).
5) Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

Tomando en cuenta la realidad de la Institución la metodología ha sido empleada cumpliendo los pasos de la siguiente manera:

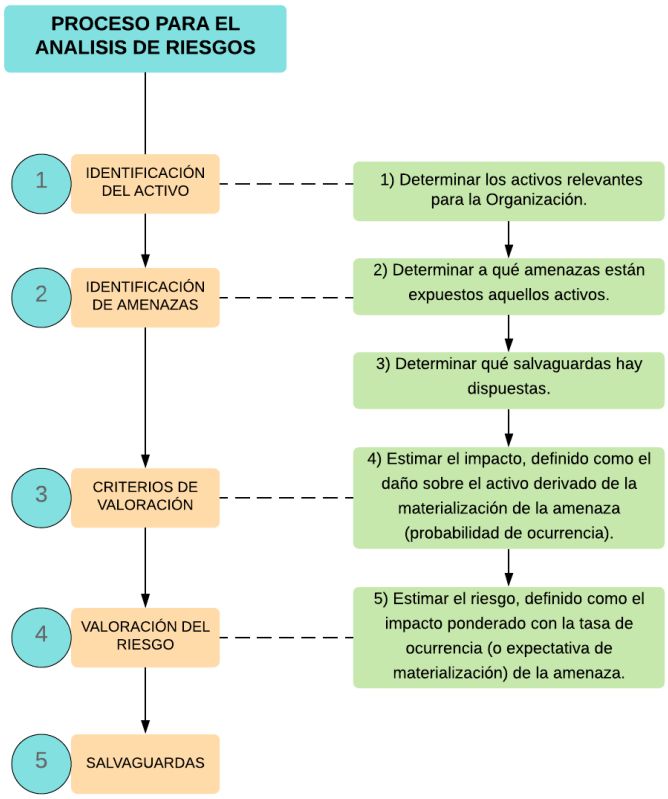


FIGURA 3: *Metodología Margerit - Proceso para realizar el Análisis de Riesgos.*

5.4.3. Metodología para la simulación del ciberataque de Ingeniería Social.

La metodología propuesta para la simulación del ciberataque de Ingeniería Social es la siguiente:

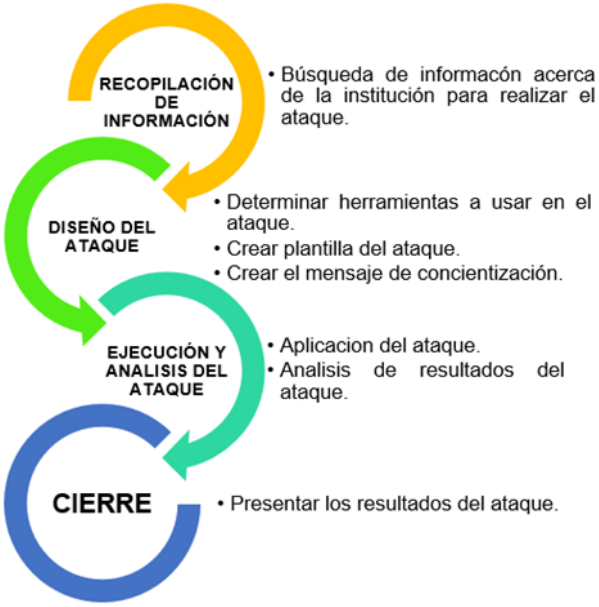


FIGURA 4: *Metodología para la simulación, propuesta por la tesista.*

5.5. Estructura del Plan Piloto

La estructura del plan piloto para mitigar los ciberataques bajo la modalidad de ingeniería social es la siguiente:

1. LIMITACIONES A LA DIVULGACIÓN DEL USO DEL INFORME.
2. ANTECEDENTES
3. ALCANCE
4. OBJETIVO
5. JUSTIFICACIÓN
6. DEFINICIONES
7. ANÁLISIS DEL RIESGO
- 7.1. IDENTIFICACIÓN DEL ACTIVO
- 7.2. IDENTIFICACIÓN DE AMENAZAS
- 7.3. CRITERIOS DE VALORACIÓN
  - 7.3.1. Probabilidad de ocurrencia
  - 7.3.2. Impacto
- 7.4. VALORACIÓN DEL RIESGO
- 7.5. CRITICIDAD DEL RIESGO
- 7.6. SALVAGUARDIAS

8. PROCESO DE ATENCIÓN A INCIDENTES
9. FORMATO PARA REPORTE DE INCIDENTES

6. RESULTADOS

En esta sección se presenta los resultados obtenidos del cumplimiento de las actividades propuestas para cada objetivo del presente Trabajo de Titulación.

FASE 1: Revisión bibliográfica entorno a la Ingeniería Social.

Para el primer objetivo del presente trabajo de titulación se aplicó el método de Revisión Sistemática de Literatura SRL basado en metodología de Bárbara Kitchenham y Brereton, esto con el fin de identificar las técnicas de ataque bajo la modalidad de Ingeniería Social y las salvaguardias (controles y contramedidas) que mitigan un ataque de esta modalidad.

6.1.1. Buscar información entorno a la Ingeniería Social.

Con la definición de los criterios de inclusión y exclusión establecidos, y con las cadenas de búsqueda establecidas en la SRL se obtuvo 28 artículos (ver TABLA 3) que aportaron en la búsqueda de información del presente TT.

TABLA 3: *Artículos seleccionados entorno a la Ingeniería Social*

COD	TITULO	AÑO
AR01	A Literature Survey on Social Engineering Attacks: Phishing Attack [42].	2016
AR02	The Social Engineering Attack Spiral (SEAS) [7]	2016
AR03	Going White Hat: Security Check by Hacking Employees Using Social Engineering Techniques [9].	2016
AR04	Social Engineering: Revisiting End-User Awareness and Susceptibility to Classic Attack Vectors.[20]	2017
AR05	Social Engineering Attack Strategies and Defence Approaches [8].	2016
AR06	Social Engineering: The Silent Attack. [6]	2015
AR07	The Awareness of Social Engineering in Information Revolution: Techniques and Challenges [15].	2015
AR08	A Layered Defense Mechanism for a Social Engineering Aware Perimeter [11].	2016
AR09	A Framework to Mitigate Social Engineering through Social Media within the Enterprise [5].	2016
AR10	Beyond Training and Awareness: From Security Culture to Security Risk Management [43].	2017
AR11	The dark side of social networking sites: Understanding phishing risks [44].	2016

AR12	Identifying Gaps in IT Retail Information Security Policy Implementation Processes [45].	2016
AR13	Countering Social Engineering through Social Media: An Enterprise Security Perspective [19].	2015
AR14	Solutions for counteracting human deception in social engineering attacks [46].	2018
AR15	Social engineering. Practice of confidential information obtained [12].	2015
AR16	Invisible Secure Keypad Solution Resilient against Shoulder Surfing Attacks [47].	2016
AR17	Social engineering as an attack vector for ransomware [48].	2017
AR18	Security Threats and Techniques in Social Networking Sites: A Systematic Literature Review [49]	2015
AR19	A client-side anti-pharming (CSAP) approach [50].	2016
AR20	Semantic analysis of dialogs to detect social engineering attacks [51].	2015
AR21	UnPhishMe: Phishing Attack Detection by Deceptive Login Simulation through an Android Mobile App [52].	2017
AR22	An Overview of Social Engineering in the Context of Information Security [40].	2018
AR23	Defending against phishing attacks: taxonomy of methods, current issues and future directions.[41]	2018
AR24	Email phishing detection and prevention by using data mining techniques [53].	2017
AR25	Phishing Environments, Techniques, and Countermeasures: A Survey [54].	2017
AR26	A literature review on phishing crime, prevention review and investigation of gaps [55].	2017
AR27	White-hat hacking framework for promoting security awareness [56].	2016
AR28	Social Engineering Prevention by Detecting Malicious URLs Using Artificial Bee Colony Algorithm [57].	2014

En base a los artículos citados se realizó la búsqueda de información que permitió identificar las técnicas (ver TABLA 4) de ataque bajo la modalidad de ingeniería social.

TABLA 4: *Técnicas de ataque.*

COD	TÉCNICAS
T01	PHISHING
T02	BAITING
T03	SMISHING
T04	QUID PRO QUO
T05	PRETEXTING
T06	PHARMING
T07	VHISHING
T08	SPEAR-PHISHING
T09	DUMPSTER DIVING
T10	SHOULDER SURFING
T11	ESPIONAJE INDUSTRIAL
T12	TAILGATING
T13	SCAREWARE

Y las salvaguardias (ver TABLA 5) para mitigar ciberataques bajo esta modalidad.

TABLA 5: *Salvaguardias*

COD	SALVAGUARDIAS
S01	Estándares
S02	Educación, Capacitación, y Concientización
S03	Técnicas de seguridad lógica
S04	Herramientas antiphishing
S05	Técnicas de autenticación
S06	Estrategias de contratación y empleo
S07	Políticas
S08	Técnicas de seguridad física
S09	Pruebas de penetración
S10	Estatutos legales
S11	Protocolos

6.1.2. Analizar la información obtenida.

La siguiente tabla muestra las técnicas y salvaguardias identificadas en los 28 artículos citados en la TABLA 3.

TABLA 6: *Técnicas de ataque y salvaguardias según cada artículo*

ART	TÉCNICAS DE ATAQUE													SALVAGUARDIAS (Métodos para mitigar)									
	T 1	T 2	T 3	T 4	T 5	T 6	T 7	T 8	T 9	T 10	T 11	T 12	T 13	S01	S02	S03	S04	S05	S06	S07	S08	S09	S10	S11
AR01	x													x	x	x	x	x						
AR02	x						x					x		x	x				x	x				x
AR03	x			x		x									x					x				
AR04	x							x							x									
AR05	x				x	x						x	x							x	x			x
AR06	x	x	x	x	x	x									x					x		x		
AR07	x			x				x	x	x					x					x			x	
AR08	x	x		x			x				x												x	
AR09	x													x	x					x				
AR10															x									
AR11	x														x							x		x
AR12	x													x	x					x				x
AR13	x					x								x	x	x				x		x		
AR14															x					x				x
AR15		x													x									
AR16										x														
AR17	x					x									x	x								
AR18	x														x	x				x			x	
AR19	x					x										x		x						
AR20	x																x	x						
AR21	x															x	x	x						

TABLA 6: *Técnicas de ataque y salvaguardias según cada artículo*

ART	TÉCNICAS DE ATAQUE													SALVAGUARDIAS (Métodos para mitigar)									
	T 1	T 2	T 3	T 4	T 5	T 6	T 7	T 8	T 9	T 10	T 11	T 12	T 13	S01	S02	S03	S04	S05	S06	S07	S08	S09	S10	S11
AR22	x	x		x	x							x			x					x	x			
AR23	x														x	x		x						
AR24	x	x			x		x	x				x				x	x							
AR25	x						x									x		x						
AR26	x														x	x	x		x					
AR27	x					x																x		
AR28	x					x												x						

Según los datos mostrados en la TABLA 6 se identificó que las técnicas de ataque bajo la modalidad de Ingeniería Social más relevantes identificadas en la SRL son: T01, T02, T04, T06; y las salvaguardias más relevantes para mitigar ciberataques bajo la modalidad de Ingeniería Social son: S02, S03, S07.

6.1.3. Documentar la información obtenida.

Los resultados de la información obtenida en la Revisión Sistemática de Literatura SRL se detallan en el ANEXO 2.

FASE 2: Simular un ciberataque bajo la modalidad de Ingeniería Social.

Para dar cumplimiento a este objetivo la Unidad de Telecomunicaciones e Información UTI y quien realizo el presente TT, firmó un acuerdo de confidencialidad (ver ANEXO 3) para proteger la identidad de los usuarios que conforman la comunidad universitaria.

Los resultados de las actividades propuestas para el cumplimiento de este objetivo se presentan a continuación.

6.2.1. Delimitar la población a quienes se enfocará el presente trabajo de titulación.

Considerando el rol que cumplen y la información que manejan por las funciones que desempeñan en la Universidad Nacional de Loja, el grupo electo al cual se enfocó el presente TT, estuvo conformado aproximadamente de 254 individuos; en base a esta población y a la fórmula del muestreo aleatorio simple, se obtuvo la siguiente muestra poblacional:

$$n = \frac{(1.96)^2 \times 0{,}5 \times 0{,}5 \times 254}{(254)(0{,}05)^2 + (1{,}96)^2(0{,}5)(0{,}5)} = \frac{243{,}9416}{1{,}5954} = 152{,}90 = 153$$

6.2.2. Identificar las principales amenazas y riesgos a los que podría estar expuesta la población, bajo la modalidad de ingeniería social.

Para el cumplimiento de esta actividad se realizó el análisis de riesgo (ver ANEXO 4) basado en la Metodología Margerit v3 (ver FIGURA 3). Mediante este análisis se identificó las técnicas mostradas en la TABLA 4 como las principales amenazas bajo la modalidad de Ingeniería Social a las cuales podrían estar expuesto el usuario. En base a las amenazas identificadas se realizó la valoración del riesgo para cada una de ellas, obteniendo los siguientes resultados:

TABLA 7: *Valoración del Riesgo de las amenazas de Ingeniería Social identificadas*.

COD	AMENAZAS	P.O.	VALORACION DEL IMPACTO			I	V.R.
			CONF.	INTE.	DISP.		
A01	PHISHING	4	4	3	1	8	**32**
A02	BAITING	2	3	3	1	7	**14**
A03	SMISHING	3	4	1	1	6	**18**
A04	Quid Pro Quo	3	3	1	1	5	**15**
A05	PRETEXTING	2	3	1	1	5	**10**
A06	PHARMING	1	3	4	1	8	**8**
A07	VHISHING	3	3	1	1	5	**15**
A08	SPEAR-PHISHING	3	4	3	1	8	**24**
A09	DUMPSTER DIVING	1	4	1	1	6	**6**
A10	SHOULDER SURFING	3	2	1	1	4	**12**
A11	ESPIONAJE INDUSTRIAL	2	3	1	1	5	**10**
A12	TAILGATING	4	4	3	3	10	**40**
A13	SCAREWARE	2	3	3	1	7	**14**

Considerando los resultados de la valoracion del riego, se identifico en el mapa de calor la zona de riesgo aceptable o inaceptable a la cual pertenece cada amenaza de Ingenieria Social.

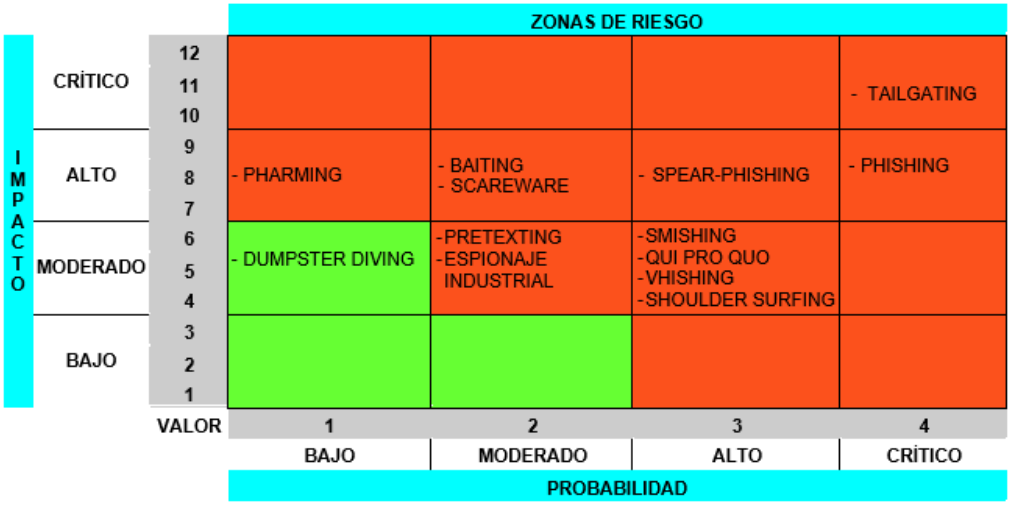


FIGURA 5: *Ubicación de las amenazas de Ingeniería Social en el mapa de calor.*

De acuerdo a los resultados de la TABLA 7 y FIGURA 5 se obtuvo que los principales riesgos a los que podría estar expuesta la población son: Phishing, Baiting,

Smishing, Quid Pro Quo, Pretexting, Pharming, Vhishing, Spear-Phishing, Shoulder Surfing, Espionaje Industrial, Tailgating, y Scareware.

6.2.3. Aplicar encuestas a la muestra poblacional, enfocadas a la Ingeniería Social.

La aplicación de la encuesta se realizó con la finalidad de determinar el conocimiento que tiene la comunidad universitaria respecto a la Ingeniería Social y del uso de la tecnología. La encuesta (ver ANEXO 5) que se utilizó para dar cumplimento a esta actividad consto de 10 preguntas y fue aplicada a un grupo de 153 personas de sexo femenino y masculino de diferente rango de edad.

6.2.4. Aplicar la simulación del ciberataque bajo la modalidad de ingeniería social a la muestra poblacional.

La técnica usada para la simulación del ataque bajo la modalidad de Ingeniería Social fue la amenaza de phishing, esto debido a los resultados obtenidos en la SRL, el análisis de riesgos, y de la encuesta aplicada. Esta amenaza se ejecutó basada en la metodología propuesta en la FIGURA 4.

6.2.4.1. RECOPILACIÓN DE LA INFORMACIÓN

a. Búsqueda de información acerca de la institución para realizar el ataque.

Para la realización de la presente simulación fue necesario conocer los correos electrónicos de las personas que serían víctimas del ciberataque.

Tomando en cuenta que en la actualidad gran parte de la información de las instituciones está ubicada en los sitios o páginas web, la recopilación de la información se realizó usando la técnica de la observación a la página web oficial de la institución www.unl.edu.ec (ver FIGURA 6), la cual al proporcionar gran cantidad de información a sus visitantes permitió obtener los correos electrónicos para realizar la simulación del ciberataque.

FIGURA 6*: Captura de la página oficial de la institución.*

Se realizó una búsqueda en internet entorno a la institución, que permitió visitar la siguiente página (ver FIGURA 7):

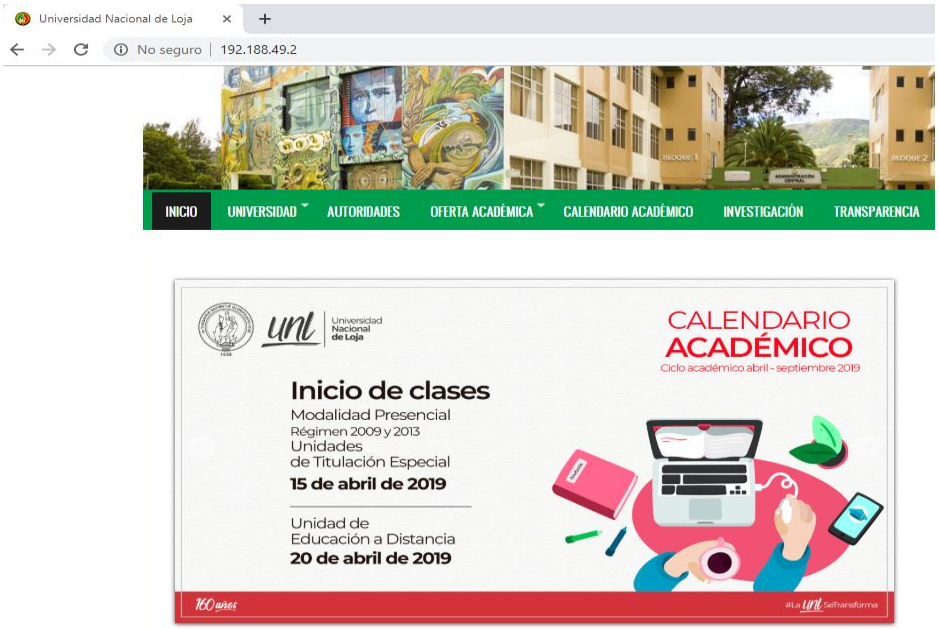


FIGURA 7: *Sitio web de la Institución con dirección IP* [*HTTP://192.188.49.2/*](HTTP://192.188.49.2/)

Además, esta página permitió conocer el formato (ver FIGURA 8) que posiblemente usa la institución para informar a la comunidad universitaria a través del correo electrónico:

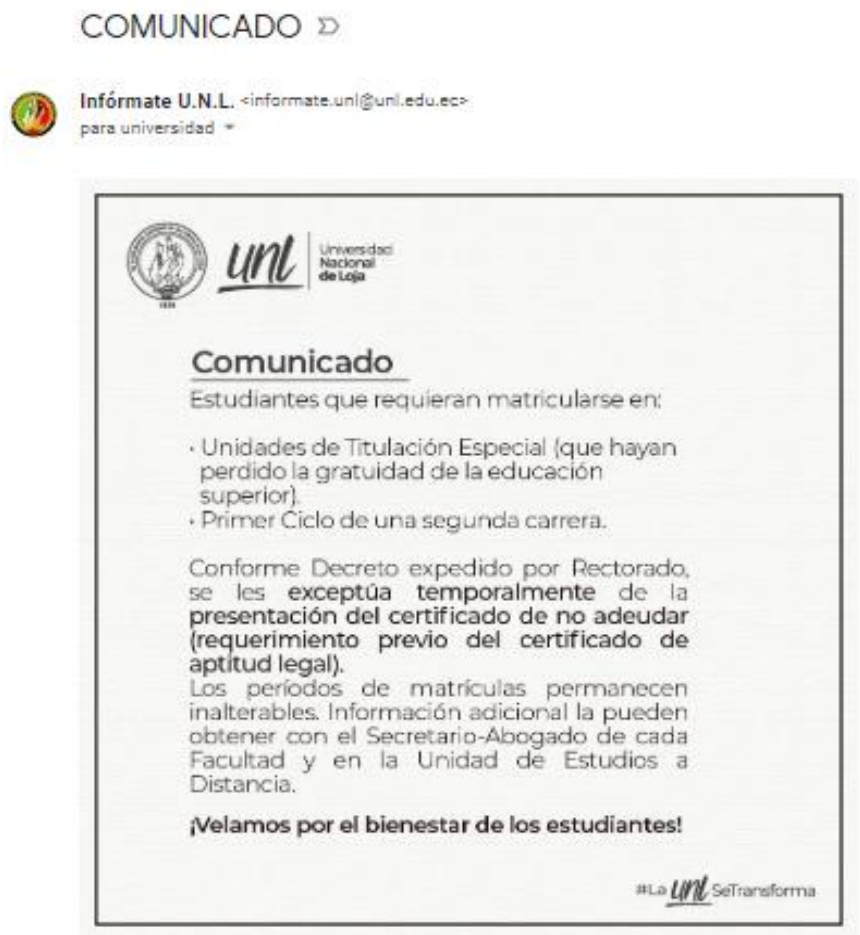


FIGURA 8: *Formato para realizar comunicados en la Institución*

6.2.4.2. DISEÑO DEL ATAQUE

a. Determinar herramientas a usar en el ataque.

Las herramientas que se empleó para la ejecución de la amenaza del phishing fueron:

- Social Engineer Toolkit - Kit de herramientas de Ingeniería Social.
- Google analitics
- Servicio de correo electrónico de Webmail
- Servicio de correo electrónico de Gmail
- Servidor Tetelsoft
- Sublime - Text
- Se utilizó el lenguaje de marcado HTML para desarrollar la plantilla de ataque y el mensaje de concientización.

b. Crear plantilla del ataque.

- Se buscó un motivo que atraiga la atención del usuario de manera que los resultados de la simulación sean satisfactorios.
- Bajo el motivo de “Calendario de Feriados Junio 2019” se desarrolló la plantilla para el ciberataque (ver FIGURA 9).

FIGURA 9: *Plantilla de ataque*

c. Crear el mensaje de concientización.

El material de concientización (ver FIGURA 10) se creó como guía para informar a los usuarios de la comunidad universitaria acerca de las amenazas de Ingeniería Social y de las Buenas Prácticas para el uso del Correo Electrónico.

FIGURA 10: *Material de concientización*

Este material de concientización fue visualizado por el usuario una vez que dio clic en el siguiente botón (ver FIGURA 11):

FIGURA 11: *Botón de enlace al material de concientización*

Nota: Para visualizar el material de concientización creado se debe ingresar en el siguiente link https://unl.edu.ec/servicios-tecnologicos/ingenieria-social

6.2.4.3. EJECUCIÓN Y ANÁLISIS DEL ATAQUE

a. Ejecución del ataque

La ejecución de la simulación se realizó cumpliendo las siguientes actividades:

- Se revisó el funcionamiento del kit de herramientas de Ingeniería Social para realizar un ataque de phishing. Se utilizó el sistema operativo Kali Linux.
- Se creó la cuenta **informate.unl@unl.edu.ec.tetelsoft.com** usando el servicio de correo electrónico de Webmail y el servidor Tetelsoft.
- Se añadió el código fuente de la plantilla de ataque y del mensaje de concientización a Google analytics, para realizar el control de cuántos usuarios revisaron el correo enviado, y cuantos visitaron el link adjunto en el correo.
- Se fragmentó por grupos los correos electrónicos institucionales de los usuarios que conforman la comunidad universitaria, y se asignó a cada grupo un código de seguimiento, el cual se añadió a la URL que redirige al usuario al mensaje de concientización.
- Debido al acuerdo de confidencialidad firmado con la institución se utilizó el método de enmascaramiento de datos para proteger la identificación de cada grupo fragmentado, quedando de la siguiente manera:

TABLA 8: *Fragmentación de correos institucionales*

GRUPO	COD	URL	DESCRIPCIÓN
A1	1001	https://unl.edu.ec/Pagina?1001	Usuarios (Muestra poblacional)
A2	1002	https://unl.edu.ec/Pagina?1002	Usuarios
B	1003	https://unl.edu.ec/Pagina?1003	Usuarios
C	1004	https://unl.edu.ec/Pagina?1004	Usuarios
D	1005	https://unl.edu.ec/Pagina?1005	Usuarios

Los correos de cada grupo fueron almacenados de 100 en 100 en un archivo .txt para su uso posterior.

La simulación se dirigió principalmente a la población delimitada (grupo A1) para dar cumplimiento a este objetivo, sin embargo, con la finalidad de obtener una mejor sustentación se ejecutó la simulación a otros usuarios que conforman los grupos A2, B, C, y D.

Finalmente, se realizó la ejecución de la simulación de la siguiente manera:

Paso 1: Se seleccionó la opción 1 “Social - Engineering Attacks”

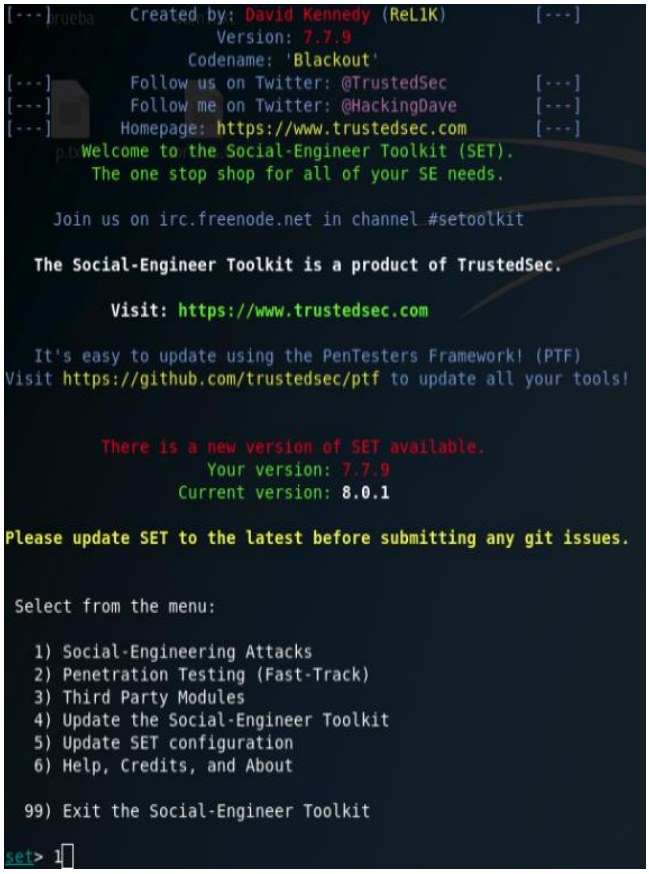


FIGURA 12: *Paso 1 - “Social - Engineering Attacks”*

Paso 2: Se seleccionó la opción 5 “Mass Mailer Attack”.

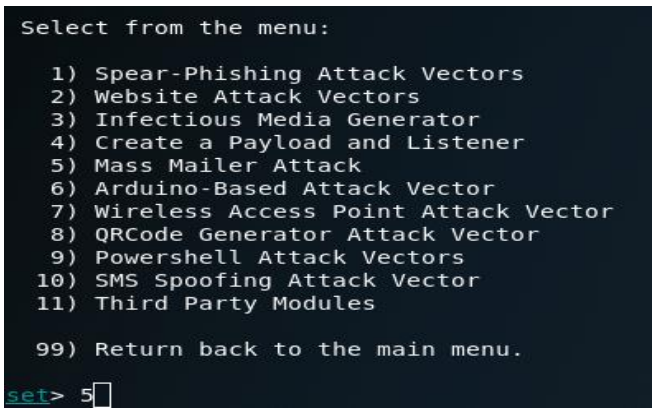


FIGURA 13: *Paso 2 - opción 5 “Mass Mailer Attack”.*

Paso 3: Se presenta la siguiente información (vere FIGURA 14) y se elige la opción 2 “E-Mail Attack Mass Mailer”.

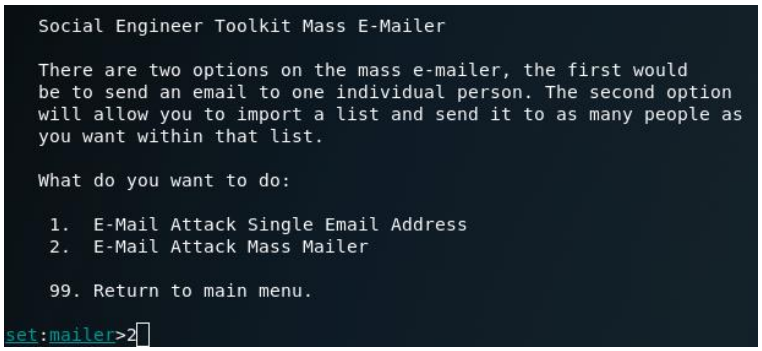


FIGURA 14: *Paso 3 - opción 2 “E-Mail Attack Mass Mailer”.*

Paso 4: Se procedió a ingresar la dirección en donde se encuentra ubicado el archivo .txt **/root/Escritorio/correos.txt** que almacenaba los correos electrónicos de los usuarios que serían víctimas de la simulación (ver FIGURA 15).

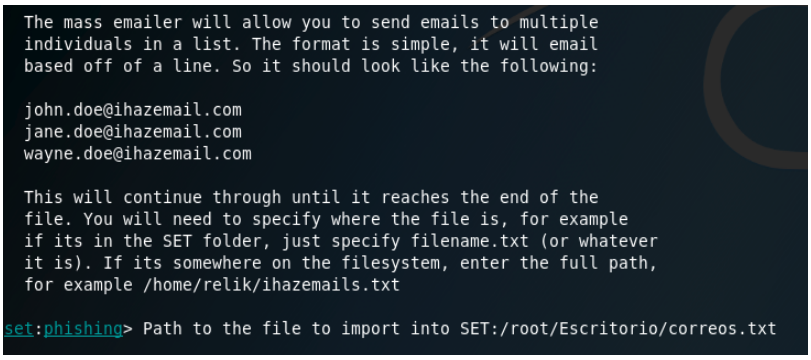


FIGURA 15: *Paso 4 – Ingreso de la dirección del archivo .txt*

Paso 5: Se seleccionó la opción 2 “Use your own server or open relay” y se procede a llenar la información (ver FIGURA 16).

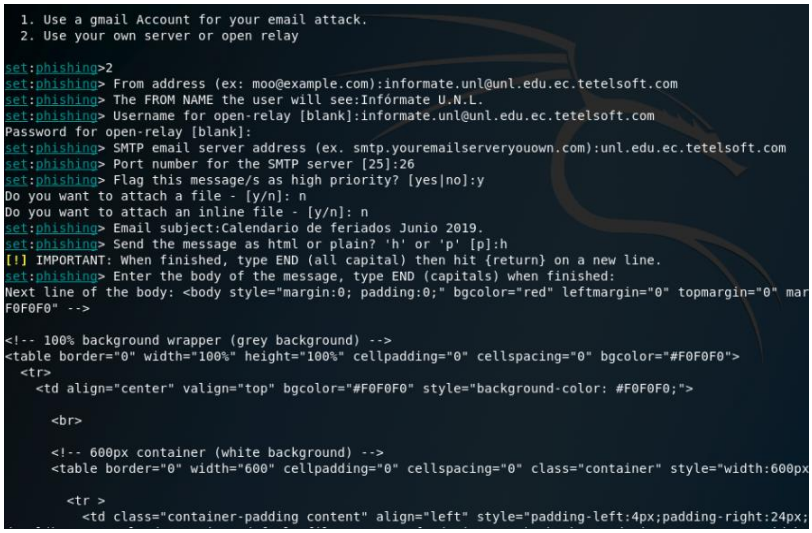


FIGURA 16: *Paso 5 - opción 2 “Use your own server or open relay”*

Pasó 6: Luego de ingresar el cuerpo del mensaje se dio doble **enter** y se escribió **END** para que el correo empiece a enviarse. (VER Figura 17)

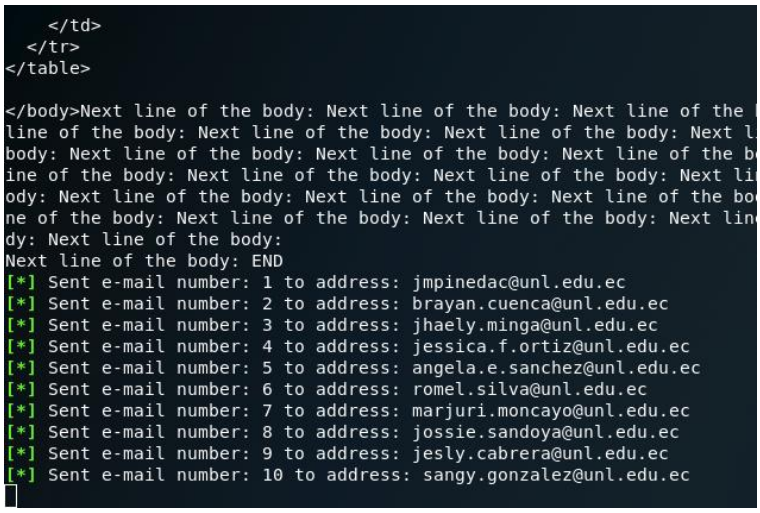


FIGURA 17: *Paso 6 – Cuerpo del mensaje*

Paso 7: Finaliza el proceso (VER Figura 18)

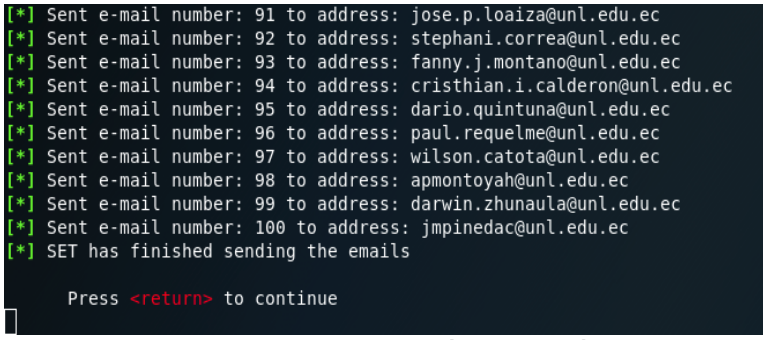


FIGURA 18: *Paso 7 – Finalización del envío de correos*

El procedimiento descrito se repitió varias veces debido a que la capacidad de correos electrónicos a los cuales se podía realizar con éxito la simulación del ciberataque era de más o menos 100 usuarios.

6.2.5. Analizar los datos obtenidos.

6.2.5.1. Análisis de los resultados obtenidos en la encuesta:

SEXO:

TABLA 9: Sexo de las personas encuestadas

SEXO	ENCUESTADOS	%
Femenino	71	46,41
Masculino	82	53,59

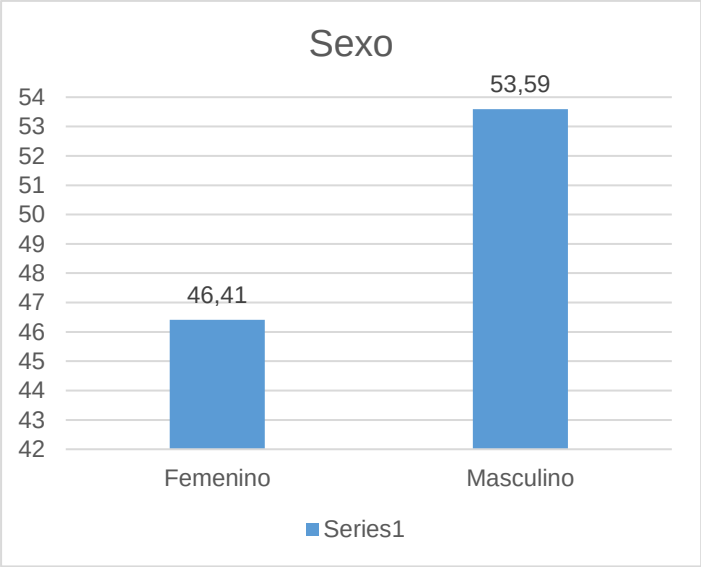


FIGURA 19: *Sexo de los encuestados*

De las 153 personas encuestadas: 71 son de sexo femenino equivalente al 46,41%, y los 82 restantes son de sexo masculino equivalente al 53,59%.

EDAD:

TABLA 10: *Rango de las edades de los encuestados*

RANGO DE EDAD	CANT	%
18 a 24 años	0	0
25 a 45 años	62	40,52
46 años en adelante	91	59,48

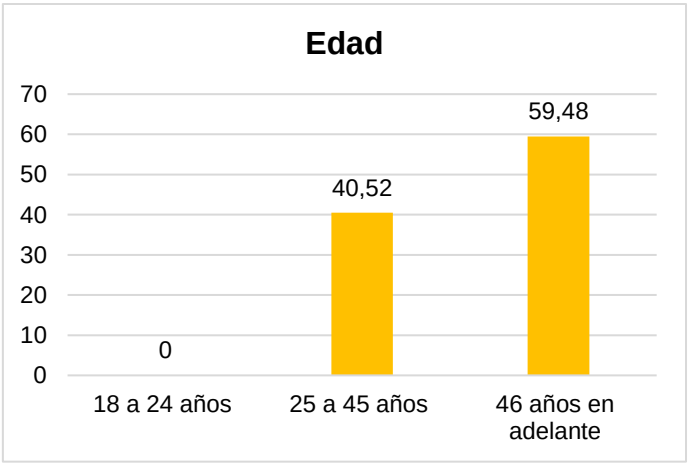


FIGURA 20: *Rango de las edades de los encuestados*

De las 153 personas encuestadas: ninguna está en el rango de 18 a 24 años, mientras que en los rangos de 25 a 45 años se tiene 62 personas equivalente al 40,52%, y en el rango de 46 años en adelante se evidencian 91 personas equivalente al 53,59%.

A continuación, se presenta el análisis de las 10 preguntas que conformaron la encuesta aplicada al grupo selecto de la comunidad universitaria.

PREGUNTA 1: ¿Cuál es el uso que usted le da al Internet?

TABLA 11: *Respuesta de la pregunta 1.*

COD	OPCIÓN	CANT	%
OP1	Trabajo	153	100
OP2	Descarga de archivos	84	54,9
OP3	Ingreso a redes sociales	64	41,83
OP4	Entretenimiento (descargar/escuchar música, ver videos videos/películas, jugar, etc)	53	34,64
OP5	Realizar compras en línea	24	15,69
OP6	Otros	9	5,88

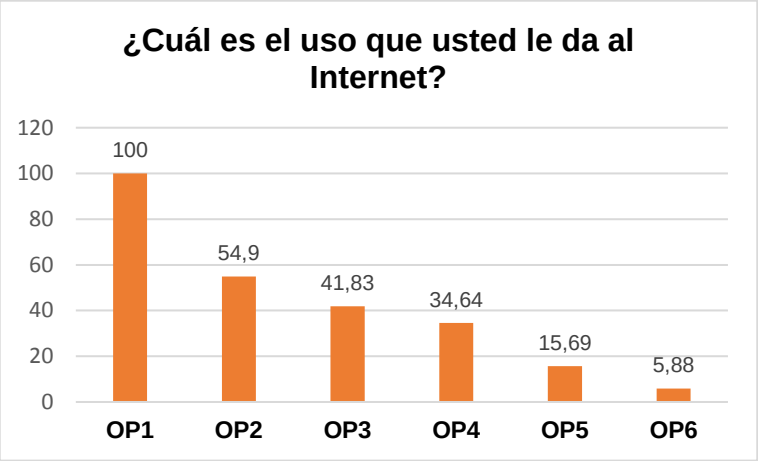


FIGURA 21: *Representación en barras de la respuesta de la pregunta 1.*

En base a la TABLA 11 y FIGURA 21 se tiene que:

- La OP1 fue marcada 153 veces, lo cual equivale al 100% de personas encuestadas.
- La OP2 fue marcada 84 veces, lo cual equivale al 54,9% del total de personas encuestadas.
- La OP3 fue marcada 64 veces, lo cual equivale al 41,83% del total de personas encuestadas.
- La OP4 fue marcada 53 veces, lo cual equivale al 34,64% del total de personas encuestadas.
- La OP5 fue marcada 24 veces, lo cual equivale al 15,69% del total de personas encuestadas.

- La OP6 en donde mencionan actividades como cursos en línea, leer temas de interés personal, o realizar investigación fue marcada 9 veces, lo cual equivale al 5,88% del total de personas encuestadas.

PREGUNTA 2: Señale el/los navegadores de internet que usted utiliza.

TABLA 12: *Respuesta de la pregunta 2*

OPCIÓN	CANT	%
Chrome	114	74,51
Firefox	78	50,98
Internet Explorer	41	26,8
Otros	6	3,92

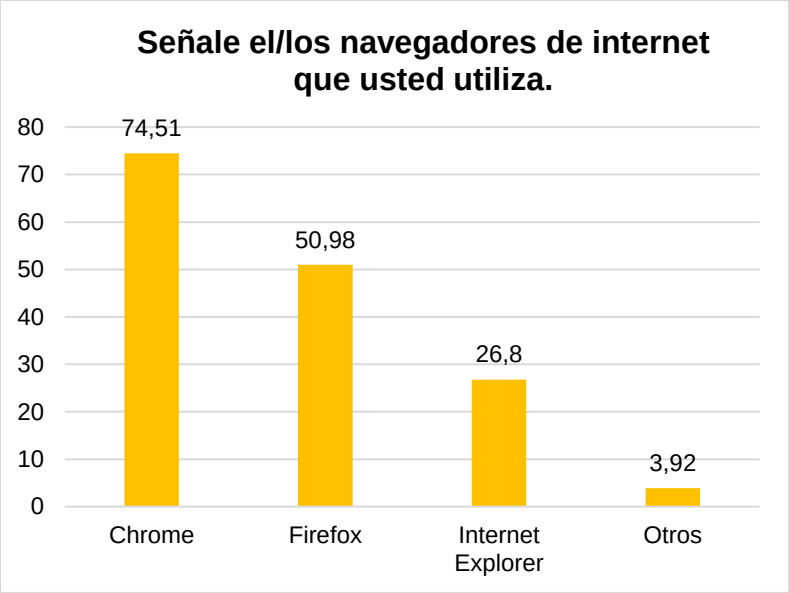


FIGURA 22: *Representación en barras de la respuesta de la pregunta 2.*

En base a la TABLA 12 y FIGURA 22 se tiene que:

- El navegador Chrome fue marcado 114 veces, lo cual equivale al 74,51% del total de personas encuestadas.
- El navegador Firefox fue marcado 78 veces, lo cual equivale al 50,98% del total de personas encuestadas.
- El navegador Internet Explorer fue marcado 41 veces, lo cual equivale al 26,8% del total de personas encuestadas.
- La opción OTROS en donde se mencionan a los navegadores como Opera, Safari, y Tarbrwoser fue marcada 6 veces, lo cual equivale al 3,92% del total de personas encuestadas.

PREGUNTA 3: ¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?

TABLA 13: *Respuesta de la pregunta 3*

COD	OPCIÓN	CANT	%
OP1	Celulares	106	69,28
OP2	Tablet	6	3,92
OP3	Portátiles	68	44,44
OP4	Computadoras de escritorio	119	77,78
OP5	Otros	1	0,65

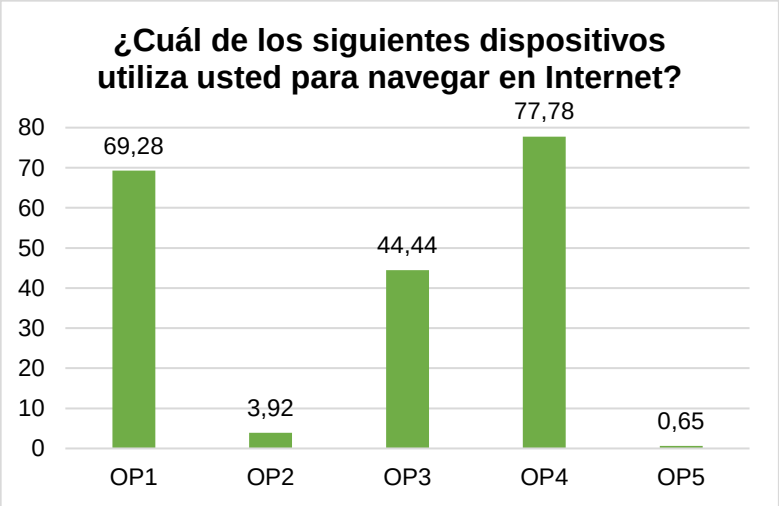


FIGURA 23: *Representación en barras de la respuesta de la pregunta 3.*

En base a la TABLA 13 y FIGURA 23 se obtiene que:

- La OP1 fue marcada 106 veces, lo cual equivale al 69,28% del total de personas encuestadas.
- La OP2 fue marcada 6 veces, lo cual equivale al 3,92% del total de personas encuestadas.
- La OP3 fue marcada 68 veces, lo cual equivale al 44,44% del total de personas encuestadas.
- La OP4 fue marcada 119 veces, lo cual equivale al 77,78% del total de personas encuestadas.
- La OP5 fue marcada 1 vez, lo cual equivale al 0,65% del total de personas encuestadas.

PREGUNTA 4: ¿Usted hace uso de las redes sociales en su lugar de trabajo?

TABLA 14: *Respuesta de la pregunta 4*

OPCIÓN	CANT	%
Si	101	66,01
No	52	33,99

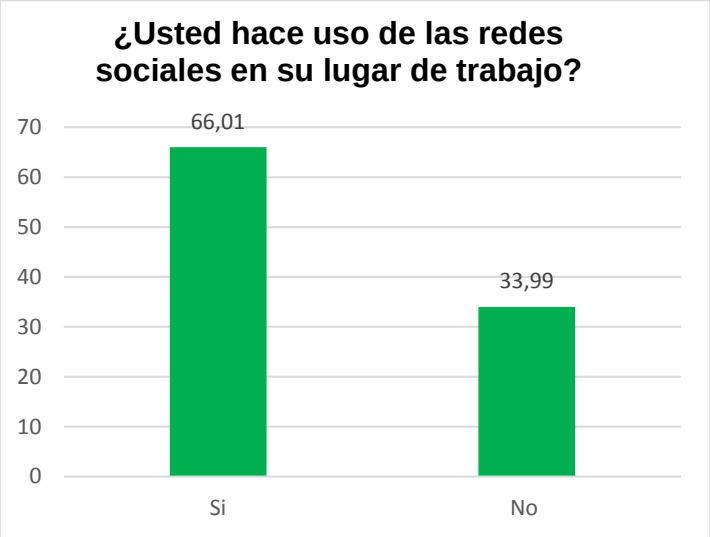


FIGURA 24: *Representación en barras de la respuesta de la pregunta 4*

De acuerdo con los resultados de la TABLA 14 y FIGURA 24 se obtiene que: de los 153 encuestados 101 personas equivalente al 66,01% respondió que **SI**, y las 52 personas restantes equivalente al 33,99% respondió que **NO**, esto, en cuanto a si el encuestado hace uso de las redes sociales en su lugar de trabajo.

Las opciones propuestas para el porcentaje de encuestados que respondieron positivamente a la presente pregunta se muestran en la siguiente tabla:

TABLA 15: *Redes Sociales*

COD	OPCIÓN	CANT	%
OP1	Facebook	53	34,64
OP2	Whatsapp	62	40,52
OP3	Twitter	13	8,50
OP4	Instagram	16	10,46
OP5	Correo Electrónico	81	52,94
OP6	Otros	2	1,31

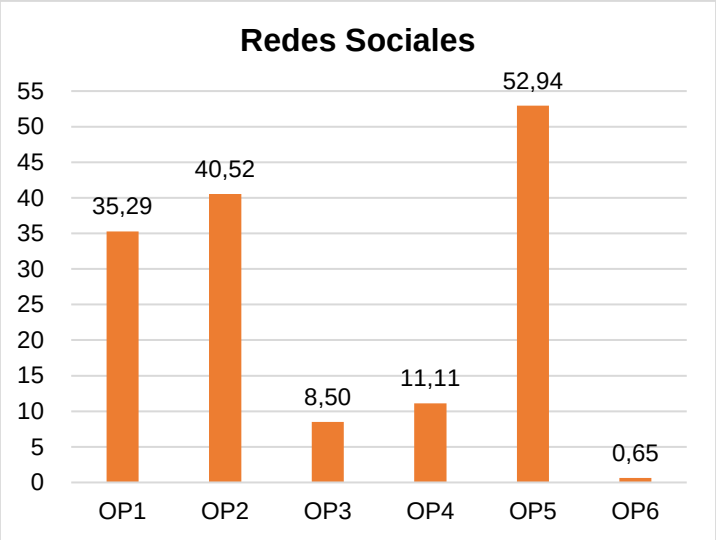


FIGURA 25: Representación en barras - Redes Sociales

Con los resultados obtenidos de la TABLA 15 y FIGURA 25 se muestra que:

- La OP1 fue marcada 53 veces, lo cual equivale al 35,29% del total de personas que respondieron **SI** a la presente pregunta.
- La OP2 fue marcada 62 veces, lo cual equivale al 40,52% del total de personas que respondieron **SI** a la presente pregunta.
- La OP3 fue marcada 13 veces, lo cual equivale al 8,50% del total de personas que respondieron **SI** a la presente pregunta.
- La OP4 fue marcada 16 veces, lo cual equivale al 11,11% del total de personas que respondieron **SI** a la presente pregunta.
- La OP5 fue marcada 81 veces, lo cual equivale al 52,94% del total de personas que respondieron **SI** a la presente pregunta.
- La OP6 fue marcada 2 veces, lo cual equivale al 0,65% del total de personas que respondieron **SI** a la presente pregunta

PREGUNTA 5: ¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas?

TABLA 16: *Respuesta de la pregunta 5*

COD	OPCIÓN	CANT	%
OP1	Mayúsculas y minúsculas	21	13,73
OP2	Mayúsculas, minúsculas y símbolos	10	6,54
OP3	Mayúsculas, minúsculas, símbolos y números	44	28,76
OP4	Mayúsculas y símbolos	3	1,96
OP5	Mayúsculas y números	14	9,15
OP6	Minúsculas y símbolos	5	3,27
OP7	Minúsculas y números	28	18,30
OP8	Símbolos y números	5	3,27
OP9	Solo mayúsculas	1	0,65
OP10	Solo minúsculas	16	10,46
OP11	Solo números	4	2,61
O12	Solo símbolos	2	1,31

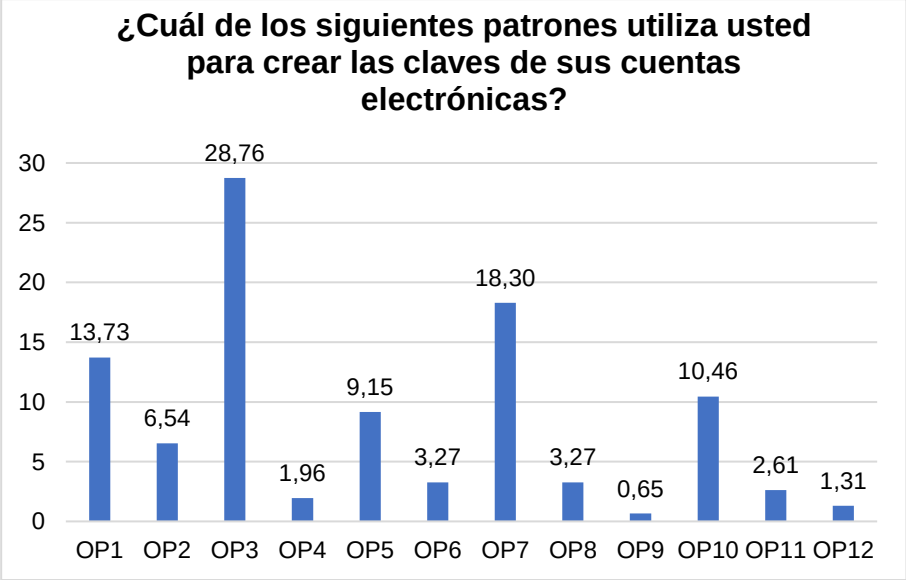


FIGURA 26: *Representación en barras de la respuesta de la pregunta 5.*

De acuerdo con los resultados de la TABLA 16 y FIGURA 26 se tiene que de las 153 personas encuestadas:

- 21 personas equivalente al 13,73% usa la OP1 como patrón para crear sus contraseñas.
- 10 personas equivalente al 6,54% usa la OP2 como patrón para crear sus contraseñas.
- 44 personas equivalente al 28,76% usa la OP3 como patrón para crear sus contraseñas.

- 3 personas equivalente al 1,96% usa la OP4 como patrón para crear sus contraseñas.
- 14 personas equivalente al 9,15% usa la OP5 como patrón para crear sus contraseñas.
- 5 personas equivalente al 3,27% usa la OP6 como patrón para crear sus contraseñas.
- 28 personas equivalente al 18,30% usa la OP6 como patrón para crear sus contraseñas.
- 5 personas equivalente al 3,27% usa la OP6 como patrón para crear sus contraseñas.
- 1 persona equivalente al 0,65% usa la OP7 como patrón para crear sus contraseñas.
- 16 personas equivalente al 10,46% usa la OP1 como patrón para crear sus contraseñas.
- 4 personas equivalente al 2,61% usa la OP1 como patrón para crear sus contraseñas.
- 2 personas equivalente al 1,31% usa la OP1 como patrón para crear sus contraseñas.

PREGUNTA 6: ¿Para que utiliza usted el correo electrónico asignado por la universidad?

TABLA 17: *Respuesta de la pregunta 6.*

COD	OPCIÓN	CANT	%
OP1	Para Trabajo	151	98,69
OP2	Para descargar archivos	22	14,38
OP3	Para entretenimiento (descargar/escuchar música, ver vídeos/películas, jugar, etc).	7	4,58
OP4	Para realizar compras en línea	2	1,31
OP5	Otros	2	1,31

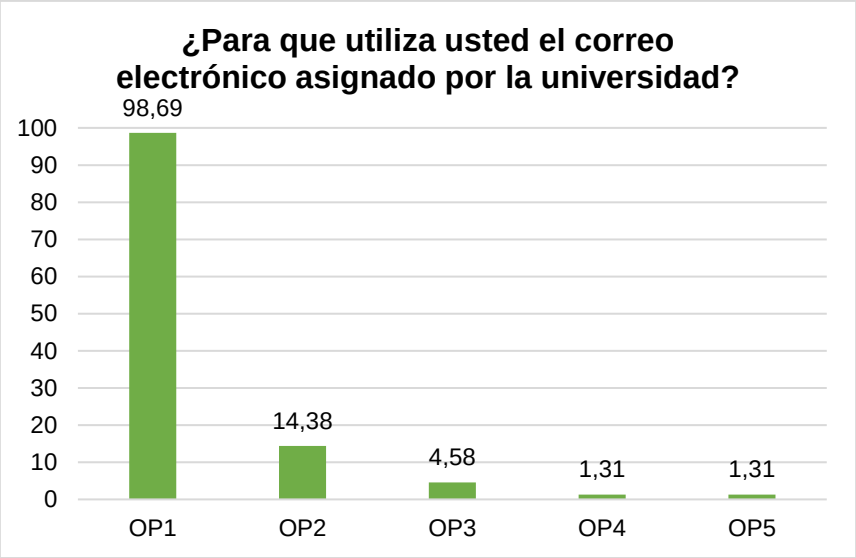


FIGURA 27: *Representación en barras de la respuesta de la pregunta 6.*

De acuerdo con los resultados de la TABLA 17 y FIGURA 27 se tiene que:

- La OP1 fue marcada 151 veces, lo cual equivale al 98,69% del total de personas encuestadas.
- La OP2 fue marcada 22 veces, lo cual equivale al 14,38% del total de personas encuestadas.
- La OP3 fue marcada 7 veces, lo cual equivale al 4,58% del total de personas encuestadas.
- La OP4 fue marcada 2 veces, lo cual equivale al 1,31% del total de personas encuestadas.
- La OP5 fue marcada 2 veces, lo cual equivale al 1,31% del total de personas encuestadas.

PREGUNTA 7: ¿Comparte usted información confidencial mediante el uso de las redes sociales?

TABLA 18: *Respuesta de la pregunta 7.*

OPCIÓN	CANT	%
Si	33	21,57
No	120	78,43

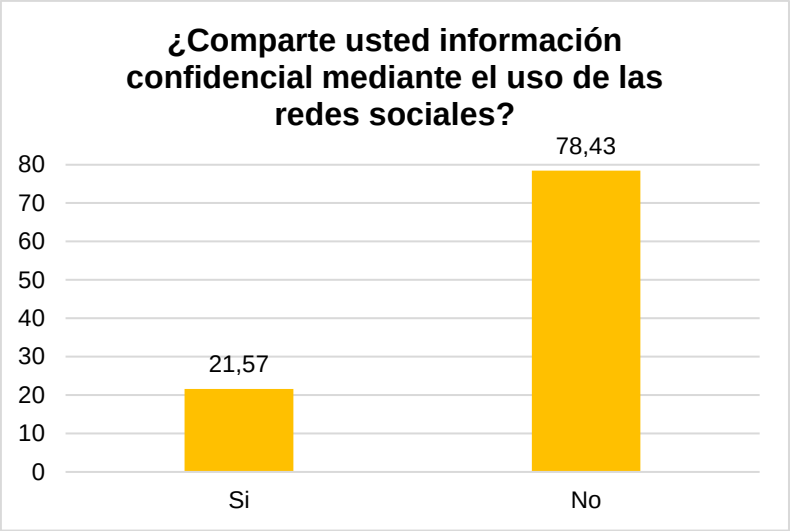


FIGURA 28: *Representación en barras de la respuesta de la pregunta 7.*

De acuerdo con los resultados de la TABLA 18 y FIGURA 28 se muestra que de los 153 encuestados 33 personas equivalente al 21,57% respondió que **SI**, y las 120 personas restantes equivalente al 78,43% respondió que **NO** comparte información confidencial mediante el uso de las redes sociales.

Los resultados de las opciones propuestas para el porcentaje de encuestados que respondieron positivamente se muestran a continuación:

TABLA 19: *Tipo de información para compartir en redes sociales*

COD	OPCIÓN	CANT	%
OP1	Claves de tarjetas de crédito	0	0
OP2	Claves de cuentas electrónicas	3	1,96
OP3	Números de cuentas bancarias	0	0
OP4	Números de tarjetas de crédito	2	1,31
OP5	Número de cédula	7	4,58
OP6	Documentos Laborales	27	17,65
OP1	Claves de tarjetas de crédito	0	0

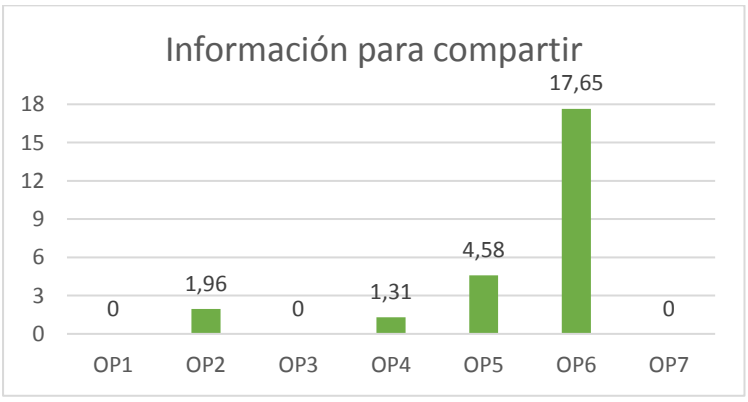


FIGURA 29*: Información para compartir en Redes Sociales.*

Con los resultados obtenidos de la TABLA 19 y FIGURA 29 tenemos que:

- La OP1, OP3, y OP7 no fueron marcadas ninguna vez.
- La OP2 fue marcada 3 veces, lo cual equivale al 1,96% del total de personas que respondieron **SI** a la presente pregunta.
- La OP4 fue marcada 2 veces, lo cual equivale al 1,31% del total de personas que respondieron **SI** a la presente pregunta.
- La OP5 fue marcada 7 veces, lo cual equivale al 4,58% del total de personas que respondieron **SI** a la presente pregunta.
- La OP6 fue marcada 27 veces, lo cual equivale al 17,65% del total de personas que respondieron **SI** a la presente pregunta.

PREGUNTA 8: ¿Conoce usted acerca de la Ingeniería Social?

TABLA 20: *Respuesta de la pregunta 8.*

OPCIÓN	CANT	%
Si	10	6,54
No	143	93,46

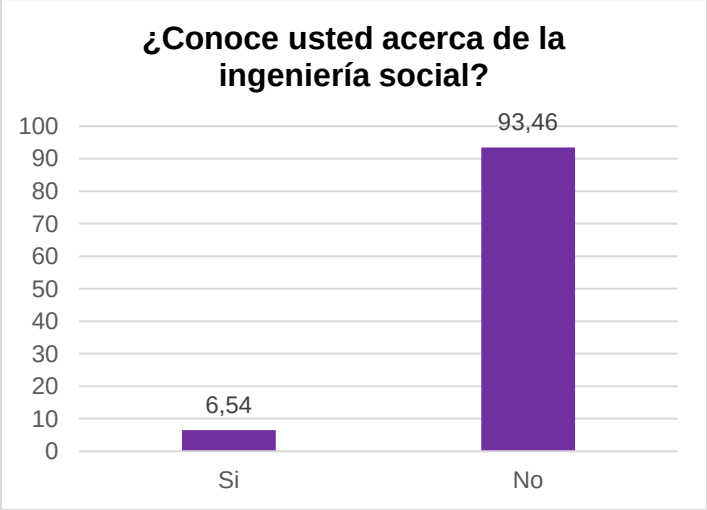


FIGURA 30*:* *Representación en barras de la respuesta de la pregunta 8.*

De acuerdo con los resultados de la TABLA 20 y FIGURA 30 se obtiene que: de los 153 encuestados 10 personas equivalente al 6,54% respondió que **SI**, y las 143 personas restantes equivalente al 93,46% respondió que **NO**, esto referente al conocimiento del encuestado acerca de la ingeniería social.

La siguiente tabla muestra los niveles “Malo, Regular, Bueno” establecidos para categorizar el conocimiento del encuestado que respondió positivamente a esta pregunta:

TABLA 21: *Nivel de conocimiento acerca de la ingeniería social.*

OPCIÓN	CANT	%
Bueno	3	3,27
Malo	2	1,96
Regular	5	1,31

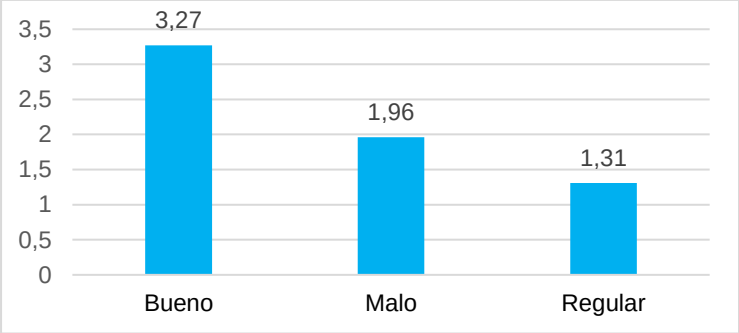


FIGURA 31*: Nivel de conocimiento del encuestado respecto a la Ingeniería Social.*

De acuerdo con la TABLA 21 y FIGURA 31, se puede concluir que, del 6,54% de encuestados que respondieron positivamente a la pregunta ¿Conoce usted acerca de la Ingeniería Social? el 3,27% tienen un buen conocimiento, el 1,96% tiene un mal conocimiento, y el 1,31% tienen un conocimiento regular.

PREGUNTA 9: ¿Conoce usted que es un delito informático?

TABLA 22: *Respuesta de la pregunta 9.*

OPCIÓN	CANT	%
Si	55	35,95
No	98	64,05

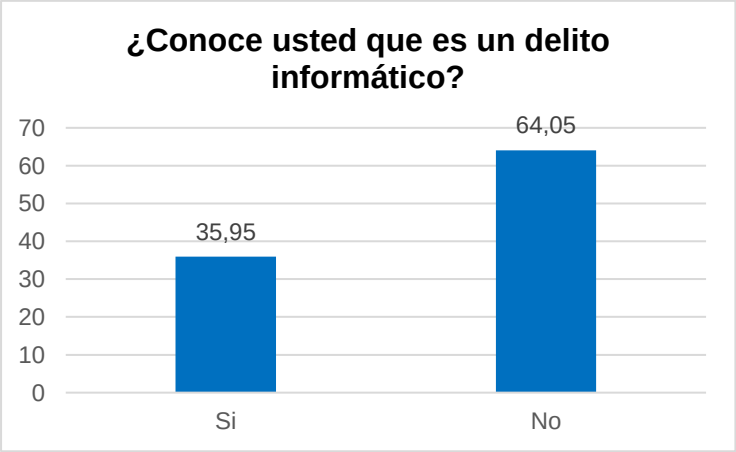


FIGURA 32*: Representación en barras de la respuesta de la pregunta 9.*

De acuerdo con los resultados de la TABLA 22 y FIGURA 32 se obtiene que de los 153 encuestados 55 personas equivalente al 35,95% respondió que **SI**, y las 98

personas restantes equivalente al 64,05% respondió que **NO**, esto referente al conocimiento del encuestado acerca de lo que es un delito informático.

La siguiente tabla muestra los niveles “Malo, Regular, Bueno” establecidos para categorizar el conocimiento del encuestado que respondió positivamente a la presente pregunta:

TABLA 23: *Nivel de conocimiento acerca de delito informático.*

OPCIÓN	CANT	%
Malo	25	16,34
Regular	14	9,15
Bueno	15	9,8

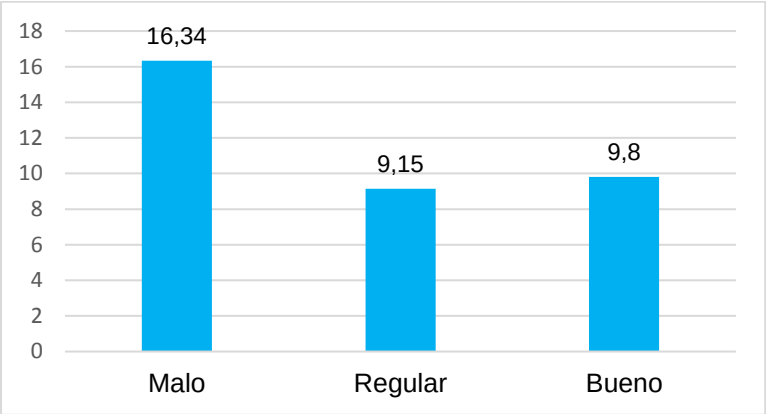


FIGURA 33: *Nivel de conocimiento acerca de delito informático*

De acuerdo con la TABLA 23 y FIGURA 33, se puede concluir que del 35,95% de encuestados que respondieron positivamente a la pregunta ¿Conoce usted que es un delito informático? el 16,34% tiene un mal conocimiento, 9,15% tiene un conocimiento regular, y el 9,8% tiene un buen conocimiento.

PREGUNTA 10: ¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?

TABLA 24: *Respuesta de la pregunta 10.*

OPCIÓN	CANT	%
Si	32	20,92
No	121	79,08

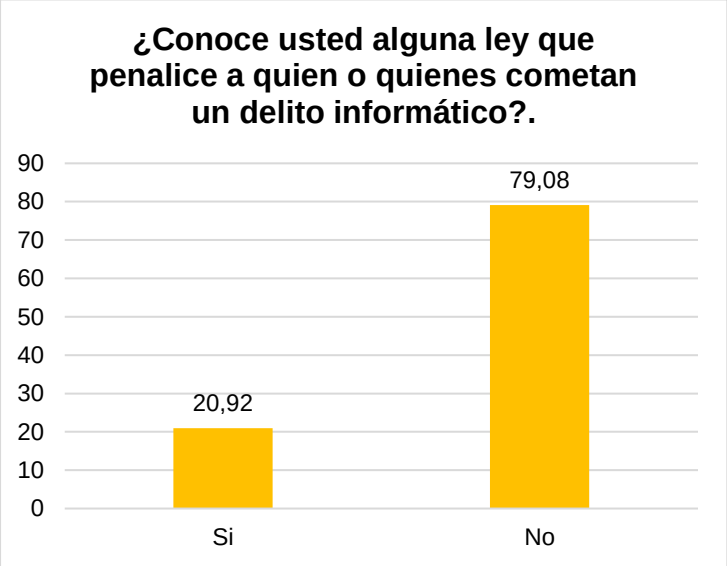


FIGURA 34*: Representación en barras de la respuesta de la pregunta 10.*

De acuerdo a los resultados de la TABLA 24 y FIGURA 34 se obtiene que: de los 153 encuestados 32 personas equivalente al 20,92% respondió que SI, y las 121 personas restantes equivalente al 79,08% respondió que NO, esto referente al conocimiento del encuestado acerca de las leyes que penalizan un delito informático.

Dentro del 20,92% de encuestados manifestaron que las leyes que penalizan un delito informático son: el Art. 103 referente a Pornografía con Menores, el Código Orgánico Integral Penal COIP, la Ley de Propiedad intelectual IEPI, la Ley Orgánica de Educación Superior LOES, la Ley de Comunicación, y la Ley de Comercio Electrónico.

6.2.5.2. Análisis de los resultados obtenidos en la simulación:

El análisis de los resultados obtenidos en la simulación (ver ANEXO 6) de la amenaza de phishing son los siguientes:

TABLA 25: *Informe de los ataques enviados*

GRUPO	COD	ATAQUES ENVIADOS	ATAQUES CON ÉXITO
A1	1001	254	215
A2	1002	100	70
B	1003	110	34
C	1004	1000	462
D	1005	1500	173

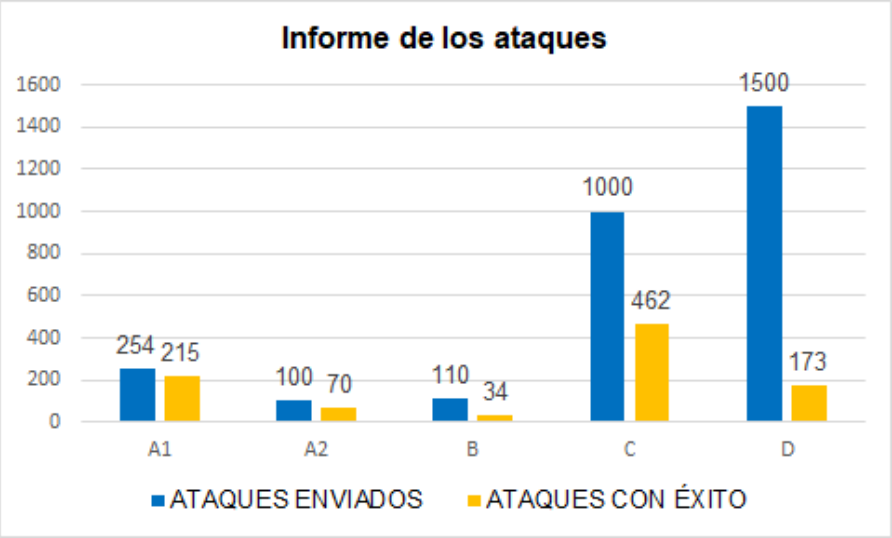


FIGURA 35*: Informe del ataque enviado*

De acuerdo a los datos mostrados en la TABLA 25 y FIGURA 35 se muestra que:

- **GRUPO A1:** De los 254 ataques enviados a los usuarios, solo 215 tuvieron éxito.
- **GRUPO A2:** De los 100 ataques enviados a los usuarios, solo 70 tuvieron éxito.
- **GRUPO B:** De los 110 ataques enviados a los usuarios, solo 34 tuvieron éxito.
- **GRUPO C:** De los 1000 ataques enviados a los usuarios, solo 462 tuvieron éxito.
- **GRUPO D:** De los 1500 ataques enviados a los usuarios, solo 173 tuvieron éxito.

6.2.6. Documentar los resultados obtenidos.

Los resultados de cada actividad propuesta para este objetivo, se han documentado como parte de la memoria del presente TT en las secciones correspondientes.

FASE 3: Desarrollar el plan piloto para mitigar los ciberataques bajo la modalidad de Ingeniería Social.

Para el cumplimiento de este objetivo primeramente se ejecutó el paso 5 del proceso de Análisis de Riesgo concerniente a las Salvaguardias y luego se desarrolló la estructura propuesta para el Plan Piloto (ver sección 5 de Materiales y Métodos). Los resultados de las actividades se presentan a continuación.

6.3.1 Establecer controles y contramedidas aplicables para disminuir los ciberataques bajo la modalidad de ingeniería social.

En base al estándar ISO/IEC 27002:2013 y tomando en cuenta las salvaguardas (ver TABLA 5) identificadas en la SRL, los controles y contramedidas para reducir o mitigar ciberataques de Ingeniería Social son las siguientes:

TABLA 26: *Controles para mitigar amenazas de Ingeniería Social.*

SALVAGUARDIAS ISO/IEC 27002:2013	
OBJETIVO DE CONTROL	**CONTROL**
5. POLÍTICAS DE SEGURIDAD	
5.1 Directrices de la Dirección en seguridad de la información	**5.1.1 Conjunto de políticas para la seguridad de la información:** Establecer políticas para la seguridad del usuario y de la información que maneja de acuerdo a las necesidades identificadas en el análisis de riesgos, las mismas que deben ser aprobadas por la dirección de TI para posteriormente ser difundidas a la toda la comunidad universitaria.
	5.1.2 Revisión de las políticas para la seguridad de la información: El departamento de TI de la institución debe definir un plan de revisiones para garantizar que las políticas cumplan con el propósito para el cual fueron creadas. El cual debe estar bajo la responsabilidad del experto en seguridad.
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	
6.1 Organización interna	**6.1.1. Asignación de responsabilidades para la seguridad de la información:** Definir y asignar de manera clara los roles y responsabilidades de cada usuario perteneciente a la comunidad universitaria.
6.1 Organización interna	**6.1.2 Segregación de tareas:** Realizar la separación de las funciones asignando distintos perfiles o áreas de responsabilidad para evitar usos o accesos indebidos a la información o a las aplicaciones o sistemas que la gestionan (activos de información) mediante la separación de las funciones asignando distintos perfiles o áreas de responsabilidad.

6.2 Dispositivos para movilidad y teletrabajo	**6.2.1 Política de uso de dispositivos para movilidad:** Para el uso de celulares, tablets, portátiles u otros dispositivos de uso personal se debe establecer una política formal y adoptar medidas de seguridad adecuadas para la protección contra los riesgos de Ingeniería Social.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	
7.1 Antes de la contratación	**7.1.1 Investigación de antecedentes:** Como parte de los métodos de reclutamiento, selección, y contratación de los nuevos docentes, administrativos, o empleados se debe realizar la verificación de antecedentes personales, académicos, laborales, penales, policiales, judiciales, y su buro de crédito.
	7.1.2 Términos y condiciones de contratación: Los acuerdos contractuales con los docentes, administrativos, empleados y terceros establecerá sus obligaciones y las obligaciones de la institución; evitando deslindarse de la responsabilidad ante un acontecimiento delictivo de Ingeniería Social.
7.2 Durante la contratación	**7.2.1 Responsabilidades de gestión:** Establecer mecanismos para asegurar que los estudiantes, docentes, administrativos, empleados y terceros actúen en concordancia con las políticas y los procedimientos establecidos la seguridad del usuario y de la información que maneja.
	7.2.2 Concienciación, educación y capacitación en seguridad de la información: Adoptar medidas como la divulgación de políticas y manuales; difusión de incidentes y ataques, explicando sus causas y orígenes; creación de talleres en materia de prevención y detección de los riesgos de ingeniería social.
	7.2.3 Proceso disciplinario: Establecer un proceso disciplinario formal para tomar medidas contra los administrativos, docentes, empleados y terceros que se han involucrado en una transgresión de ingeniería social.
7.3 Cese o cambio de puesto de trabajo.	**7.3.1 Cese o cambio de puesto de trabajo:** Establecer mecanismos devolución de activos y eliminación de los derechos de acceso físico y lógicos ante el abandono o cambio de puesto por parte de los docentes, administrativos, o empleados.

8. GESTIÓN DE ACTIVOS	
8.1 Responsabilidad sobre los activos	**8.1.1 Inventario de activos:** Se deben identificar los activos o recursos asociados al usuario.
	8.1.3 Uso aceptable de los activos: Se debe identificar, documentar e implementar reglas para el buen uso de los activos o recursos asociados al usuario.
8.2 Clasificación de la información	**8.2.1. Directrices de clasificación:** Establecer métodos para la clasificación de la información en función de la integridad, confidencialidad y disponibilidad de la misma.
	8.2.2 Etiquetado y manipulado de la información: Establecer procedimientos para el etiquetado de acuerdo al esquema de clasificación de información adoptado por la institución.
	8.2.3 Manipulación de activos: Establecer procedimientos para la manipulación de la información de acuerdo al esquema de clasificación adoptado por la institución.
8.3 Manejo de los soportes de almacenamiento	**8.3.1 Gestión de soportes extraíbles:** Se debe restringir la conexión de celulares, tablets, portátiles, USB u otros dispositivos removibles de uso personal a la red de la institución sin la debida autorización.
9. CONTROL DE ACCESOS.	
9.2 Gestión de acceso de usuario	**9.2.1 Gestión de altas/bajas en el registro de usuarios:** Implementar métodos de registro y cancelación de accesos de un usuario, desde el registro inicial hasta su baja cuando ya no sea necesario su acceso.
	9.2.2 Gestión de los derechos de acceso asignados a usuario: Establecer procedimientos de control de acceso físico y lógico para los usuarios, con el fin de asegurar que los activos de información se mantengan protegidos.
	9.2.5 Revisión de los derechos de acceso de los usuarios: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.

	9.2.6 Retirada o adaptación de los derechos de acceso: Los derechos de acceso para todos estudiantes, docentes, administrativos, empleados y usuarios externos a la información y a las instalaciones se deberían eliminar al término de su empleo, contrato o acuerdo, o se deberían ajustar en caso de realizarse cambios en el empleo.
9.3 Responsabilidades del usuario.	**9.3.1 Uso de información confidencial para la autenticación:** La autenticación de cada usuario (estudiante, docente, administrativo, empleado, o tercero) para el ingreso a las instalaciones, información, sistemas, etc. debe ser única y no puede ser compartida.
9.4 Control de acceso a sistemas y aplicaciones.	**9.4.1. Restricción del acceso a la información:** El acceso a la información de la institución se debe restringir de acuerdo con la política de control de acceso establecida previamente.
	9.4.2. Procedimientos seguros de inicio de sesión: Establecer buenas prácticas de seguridad para el uso y protección de claves o contraseñas, las cuales constituyen un medio de validación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos de manera segura.
	9.4.5 Control de acceso al código fuente de los programas: El departamento de TI de la institución debe establecer mecanismos de protección para el código fuente de sus aplicativos desarrollados.
11. SEGURIDAD FÍSICA Y AMBIENTAL.	
11.1 Áreas seguras	**11.1.1 Perímetro de seguridad física:** Definir perímetros de seguridad para la protección de las áreas que contienen información confidencial o critica.
	11.1.2 Controles físicos de entrada: Implementar sensores de identificación como: analizadores de retina, tarjetas inteligentes, video cámaras, vigilantes jurados, etc. para acceder a las diferentes dependencias de la institución.

	11.1.3 Seguridad de oficinas, despachos y recursos: Diseñar y aplicar un sistema de seguridad física a las oficinas, salas e instalaciones de la organización.
11.2 Seguridad de los equipos.	**11.2.1 Emplazamiento y protección de equipos:** Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas de ingeniería social.
	11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla: Adoptar una política para evitar el acceso no autorizado a la información en los puestos de trabajo, como también a las instalaciones y a los equipos compartidos.
12. SEGURIDAD EN LA OPERATIVA.	
12.2 Protección contra código malicioso.	**12.2.1 Controles contra el código malicioso:** Establecer controles de detección y prevención contra el malware o código malicioso.
13. SEGURIDAD EN LAS TELECOMUNICACIONES.	
13.1 Gestión de la seguridad en las redes.	**13.1.1 Controles de red:** Establecer mecanismos (Configuraciones Seguras de Dispositivos de Red: Firewalls, Routers y Switches) para administrar y controlar las redes para proteger la información en sistemas y aplicaciones.
	13.1.2 Mecanismos de seguridad asociados a servicios en red: Se debe identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.
13.2 Intercambio de información con partes externas.	**13.2.1 Políticas y procedimientos de intercambio de información:** Establecer políticas, procedimientos y controles para proteger la transferencia de información mediante el uso de todo tipo de dispositivos de comunicación.
	13.2.2 Acuerdos de intercambio: Crear acuerdos para tratar la transferencia segura de información entre la institución y las partes externas.

	13.2.3 Mensajería electrónica: Emplear la política para el buen uso del correo electrónico desarrollada por la Unidad de Telecomunicaciones e Información de la Universidad. Además, se debe desarrollar una guía de buenas prácticas para el reconocimiento de ataques de phishing.
18. CUMPLIMIENTO.	
18.1 Cumplimiento de los requisitos legales y contractuales.	**18.1.1 Identificación de la legislación aplicable:** La legislación aplicable para tomar acciones entorno a la Ingeniería Social en la institución son: ✓ El Esquema Gubernamental de Seguridad de la Información EGSI. ✓ Las Políticas de Telecomunicaciones, Desarrollo de Software, Redes de La Universidad Nacional de Loja. ✓ La Ley de Comercio Electrónico, Firmas y Mensajes de Datos. ✓ Código Orgánico Integral Penal COIP. Los mismos que deben estar documentados y actualizados.
	18.1.2 Derechos de propiedad intelectual (DPI): Supervisar que el uso del software, la información propia de la institución o adquirida de terceros, y los aplicativos desarrollados estén de acuerdo a la Ley de Propiedad Intelectual del Ecuador.
	18.1.3 Protección de los registros de la organización: Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos.
	18.1.4 Protección de datos y privacidad de la información personal: Establecer una política para la protección de datos y privacidad de la información personal en base al modelo europeo de la Ley Orgánica de Protección de Datos Personales.

Teniendo en cuenta lo anterior descrito, la siguiente tabla muestra los controles y contramedidas que mitigan a cada amenaza de Ingeniería Social identificada:

TABLA 27: *Controles para mitigar cada amenaza de Ingeniería Social identificada.*

SALVAGUARDIAS ISO/IEC 27002:2013														
OBJETIVO DE CONTROL	**CONTROL**	**AMENAZAS DE INGENIERÍA SOCIAL**												
		A 01	**A 02**	**A 03**	**A 04**	**A 05**	**A 06**	**A 07**	**A 08**	**A 09**	**A 10**	**A 11**	**A 12**	**A 13**
5. POLÍTICAS DE SEGURIDAD														
5.1 Directrices de la Dirección en seguridad de la información	5.1.1 Conjunto de políticas para la seguridad de la información	x	x	x	x	x	x	x	x	x	x	x	x	x
	5.1.2 Revisión de las políticas para la seguridad de la información	x	x	x	x	x	x	x	x	x	x	x	x	x
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN														
6.1 Organización interna	6.1.1. Asignación de responsabilidades para la seguridad de la información.	x	x	x	x	x	x	x	x	x	x	x	x	x
	6.1.2 Segregación de tareas	x	x	x	x	x	x	x	x	x	x	x	x	x
6.2 Dispositivos para movilidad y teletrabajo	6.2.1 Política de uso de dispositivos para movilidad		x	x				x						

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.														
7.1 Antes de la contratación	7.1.1. Investigación de antecedentes.					x					x	x		
	7.1.2 Términos y condiciones de contratación.											x		
7.2 Durante la contratación	7.2.1 Responsabilidades de gestión.	x	x	x	x	x	x	x	x	x	x	x	x	x
	7.2.2. Concienciación, educación y capacitación en seguridad de la información.	x	x	x	x	x	x	x	x	x	x	x	x	x
7.3 Cese o cambio de puesto de trabajo	7.2.3 Proceso disciplinario.	x	x	x	x	x	x	x	x	x	x	x	x	x
	7.3.1 Cese o cambio de puesto de trabajo.											x		
8. GESTIÓN DE ACTIVOS														
8.1 Responsabilidad sobre los activos	8.1.1 Inventario de activos.	x	x	x	x	x	x	x	x	x	x	x	x	x
	8.1.3 Uso aceptable de los activos.	x	x	x	x	x	x	x	x	x	x	x	x	x
8.2 Clasificación de la información	8.2.1 Directrices de clasificación.	x	x	x	x	x	x	x	x	x	x	x	x	x
	8.2.2 Etiquetado y manipulado de la información.	x	x	x	x	x	x	x	x	x	x	x	x	x
	8.2.3 Manipulación de activos.	x	x	x	x	x	x	x	x	x	x	x	x	x
8.3 Manejo de los soportes de almacenamiento.	8.3.1 Gestión de soportes extraíbles.		x											

9. CONTROL DE ACCESOS.														
9.2 Gestión de acceso de usuario	9.2.1 Gestión de altas/bajas en el registro de usuarios.											x		
	9.2.2 Gestión de los derechos de acceso asignados a usuarios.		x			x				x		x	x	
	9.2.5 Revisión de los derechos de acceso de los usuarios.											x		
	9.2.6 Retirada o adaptación de los derechos de acceso.											x		
9.3 Responsabilidades del usuario.	9.3.1 Uso de información confidencial para la autenticación.	x		x				x	x	x	x	x		
9.4 Control de acceso a sistemas y aplicaciones.	9.4.1. Restricción del acceso a la información	x		x	x	x		x	x	x	x	x	x	
	9.4.2. Procedimientos seguros de inicio de sesión	x		x					x		x	x	x	
	9.4.5 Control de acceso al código fuente de los programas.							x						

11. SEGURIDAD FÍSICA Y AMBIENTAL.														
11.1 Áreas seguras	11.1.1 Perímetro de seguridad física.		x							x	x	x	x	
	11.1.2 Controles físicos de entrada.		x							x	x	x	x	
	11.1.3 Seguridad de oficinas, despachos y recursos.		x							x	x	x	x	
11.2 Seguridad de los equipos.	11.2.1 Emplazamiento y protección de equipos.		x											
	11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.		x						x	x	x	x	x	
12. SEGURIDAD EN LA OPERATIVA.														
12.2 Protección contra código malicioso.	12.2.1 Controles contra el código malicioso.	x	x				x		x					x

13. SEGURIDAD EN LAS TELECOMUNICACIONES.														
13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red.						x							
	13.1.2 Mecanismos de seguridad asociados a servicios en red.	x					x		x					
13.2 Intercambio de información con partes externas.	13.2.1 Políticas y procedimientos de intercambio de información.	x		x	x	x		x	x			x		
	13.2.2 Acuerdos de intercambio.	x		x	x	x		x	x			x		
	13.2.3 Mensajería electrónica	x							x					
18. CUMPLIMIENTO														
18.1 Cumplimiento de los requisitos legales y contractuales.	18.1.1. Identificación de la legislación aplicable.													
	18.1.2. Derechos de propiedad intelectual (DPI)													
	18.1.3 Protección de los registros de la organización.													
	18.1.4 Protección de datos y privacidad de la información personal.													

6.3.2. Crear el plan piloto para mitigar los ciberataques bajo la modalidad de ingeniería social.

Para el cumplimiento de esta actividad se procedió a desarrollar cada sección de la estructura propuesta para el Plan Piloto.

1. LIMITACIONES A LA DIVULGACIÓN DEL USO DEL INFORME

Este documento contiene información de uso interno y está destinado exclusivamente para los estudiantes, docentes, administrativos y empleados de la Universidad Nacional de Loja. En este informe se detallan las amenazas de Ingeniería Social a las que podría estar expuesta la comunidad universitaria, así como las posibles salvaguardias (controles y contramedidas) para ser mitigadas.

2. ANTECEDENTES

CONSIDERANDO QUE:

La "LEY ORGANICA DEL SISTEMA NACIONAL DE REGISTRO DE DATOS PUBLICOS", en su capítulo 2, respecto a los PRINCIPIOS GENERALES DEL REGISTRO DE DATOS PUBLICOS específicamente en el Art. 4.- Responsabilidad de la información.

"(..) ***Art. 4.- Responsabilidad de la información. -*** *Las instituciones del sector público y privado (…), son responsables de la integridad, protección y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros (…)"*

El "ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN EGSI", en su sección 4, respecto a la SEGURIDAD DE LOS RECURSOS HUMANOS específicamente en los puntos 4.4. Responsabilidades de la dirección a cargo del funcionario, 4.5. Educación, formación y sensibilización en seguridad de la información establece lo siguiente:

"(...) ***4.4. Responsabilidades de la dirección a cargo del funcionario.*** *(...) b) Lograr la concienciación sobre la seguridad de la información correspondiente a sus funciones y responsabilidades dentro de la institución. c) Acordar los términos y las condiciones laborales, las cuales incluyen la política de la*

seguridad de la información de la institución y los métodos apropiados de trabajo. (...) ”

“(...) ***4.5. Educación, formación y sensibilización en seguridad de la información.*** *a) Socializar y capacitar de forma periódica y oportuna sobre las normas y los procedimientos para la seguridad, las responsabilidades legales y los controles de la institución, así como en la capacitación del uso correcto de los servicios de información. “*

Las “POLÍTICAS DE TELECOMUNICACIONES, DESARROLLO DE SOFTWARE, REDES” de la Universidad Nacional de Loja aprobadas bajo resolución Nro. 019/2013-R-UNL el 9 de mayo de 2013 en su sección 1, respecto a las POLÍTICAS UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN específicamente en las Políticas de Administración de Recursos, Políticas de Salvaguarda y Confidencialidad, Políticas de protección de datos y sistemas establecen lo siguiente:

“(…) ***1.2. Políticas de administración de recursos.*** *(...) La UTI deberá proveer los mecanismos de protección y controles necesarios que aseguren la integridad y privacidad de los datos almacenados en los archivos y bases de datos que tenga en custodia (…)”.*

“(...) ***1.5. Políticas de Salvaguarda y Confidencialidad.*** *Los funcionarios de la UTI bajo cualquier forma de estructura, se comprometen a salvaguardar de todo riesgo y a guardar la más absoluta reserva y/o confidencialidad sobre toda la información, cualquiera sea su naturaleza (...) “*

“ ***1.6. Políticas de Protección de datos y sistemas****. (...) queda prohibido al usuario realizar intervenciones no debidas, entre las que se encuentran:*

- *Manipulación no autorizada.*
- *Apertura, reemplazo y/o desconexión de componentes.*
- *Reasignaciones permanentes o temporales sin autorización.*
- *Instalación de programas, sistemas, módulos y/o archivos externos.*
- *Empleo de juegos y/o programas con fines no laborales.*
- *Modifica la configuración de sistemas, programas o dispositivos.*
- *Desinstalar sistemas, programas, módulos oficiales de la Universidad Nacional de Loja.*

- *Conexión a redes eléctricas o de Datos no certificadas y o autorizadas. (...)"*

"LAS POLÍTICAS DE TELECOMUNICACIONES, DESARROLLO DE SOFTWARE, REDES" de la Universidad Nacional de Loja aprobadas bajo resolución Nro. 019/2013-R-UNL el 9 de mayo de 2013 en su sección 5, respecto a las POLÍTICAS DE LA SECCIÓN DE REDES Y EQUIPOS INFORMÁTICOS específicamente en las Políticas de uso de red, y Obligaciones del Usuario establecen lo siguiente:

(...) ***5.4. Políticas de uso de red.*** *(...) Es responsable el usuario por los sitios que visite en internet; El usuario es responsable de la información (audio, video, documentos, etc.) que baje de Internet o Intranet (...); (...) Los usuarios gozan de privacidad de su información, con la excepción de aquellos en los que se detecten acciones que pongan en riesgo la seguridad de la red del campus universitario. (...)*

(...) ***5.6. Obligaciones del Usuario.*** *(...) El alumno, docente o empleado es completamente responsable de todas las actividades realizadas con su cuenta de correo proporcionada por la UTI.*

(...)(...) El buen uso de su cuenta se entiende por:

- *Usar su cuenta con fines académicos y/o investigación.*
- *Respetar las cuentas de otros usuarios.*
- *No mandar ni contestar cadenas de correo.*
- *No usar su cuenta para fines comerciales.*
- *No enviar material obsceno o con intención de intimidar, insultar o acosar (...)"*

Se elabora el presente documento para mitigar los ciberataques de Ingeniería Social en la Universidad Nacional de Loja, el cual servirá de guía para resguardar y proteger al usuario o institución y a su información.

3. ALCANCE

Este documento y sus directrices aplican para todos los estudiantes, docentes, administrativos y empleados de la Universidad Nacional de Loja con el fin de mitigar ciberataques de Ingeniería Social.

4. OBJETIVO

Difundir las políticas y estándares de seguridad a la comunidad universitaria para mitigar los ciberataques de Ingeniería Social, y salvaguardar la información de los usuarios y de la institución.

5. JUSTIFICACIÓN

La aplicación de encuestas y la simulación de una de las amenazas más latentes de Ingeniería Social a un grupo (usuario: estudiantes, docentes, administrativos, o empleados) seleccionado de la comunidad universitaria permitieron identificar que el usuario es vulnerable a ser víctima a ciberataques bajo esta modalidad.

Una vez conocida la realidad de la institución y considerando los lineamientos del "ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN EGSI" y "LAS POLÍTICAS DE TELECOMUNICACIONES, DESARROLLO DE SOFTWARE, REDES" de la Universidad Nacional de Loja, La Unidad Telecomunicaciones e Información ha visto óptimo desarrollar este documento para establecer controles y contramedidas de seguridad, que permitan resguardar y proteger al usuario o institución y a su información.

6. DEFINICIONES

Los términos y definiciones aplicables para el desarrollo de este documento se basan en Magerit v3, y la Norma ISO/IEC 27002:2013.

- **Magerit v3:** Es la metodología utilizada para realizar el análisis de riesgos.
- **ISO/IEC 27002-2013:** Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad del usuario.

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la institucion.
- **Amenaza:** Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización.

- **Análisis de riesgos:** Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.
- **Antivirus:** Programa diseñado para detectar, detener y eliminar códigos maliciosos (virus, troyanos, gusanos, etc.), así como proteger los equipos de otros programas peligrosos conocidos genéricamente como malware.
- **Atacante:** Es la persona que realiza el ciberataque de ingeniería social
- **Ciberseguridad:** Protección de dispositivos, servicios o redes, así como la protección de datos frente a intentos de robo o daño.
- **Contramedida:** Son aquellos procedimientos o mecanismos utilizados para protegerse de una amenaza.
- **Control:** Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.
- **Impacto:** Es la medida del daño sobre el activo derivado de la materialización de una amenaza.
- **Incidente:** Hecho o evento que puede afectar un activo de información.
- **Ingeniería social:** Técnicas utilizadas para manipular a la gente a fin de que realice acciones específicas o se sume a la difusión de información que es útil para un atacante.
- **Malware:** Software que hace referencia a todos los programas o códigos informáticos cuya función es dañar o causar el mal funcionamiento de un sistema.
- **Riesgo:** Es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.
- **Seguridad de la Información:** Medidas de protección enfocadas a preservar la confidencialidad, integridad y disponibilidad de la información.
- **Vulnerabilidad:** Es toda debilidad que puede ser aprovechada por una amenaza, es decir que son las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial.

7. ANÁLISIS DEL RIESGO

Los resultados de esta sección se encuentran desarrollados en el ANEXO 4.

8. PROCESO DE ATENCIÓN A INCIDENTES

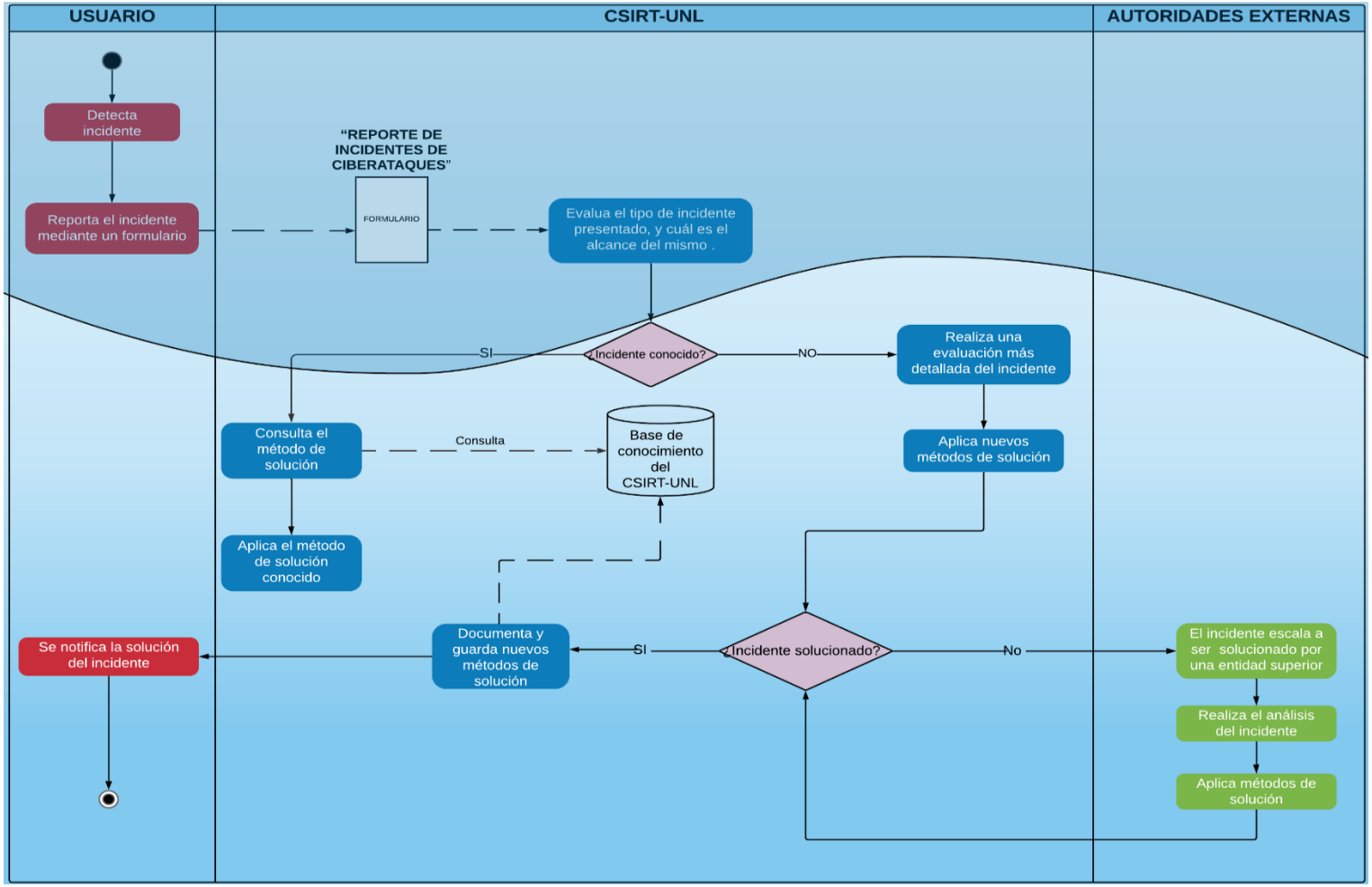


FIGURA 36: *Flujograma de manejo de incidentes*

El usuario quien está representado por los estudiantes, docentes, administrativos, o empleados es quien detecta el incidente de Ingeniería Social el cual puede ser realizado de manera presencial o a través del correo electrónico, llamadas telefónicas, mensajes de texto, etc.

Para reportar el incidente el usuario deberá llenar y enviar el formulario de **"REPORTE DE INCIDENTES DE CIBERATAQUES**" que se encuentra colgado en el sitio web www.csirt.unl.edu.ec el mismo que será receptado por el CSIRT-UNL quien se encargara de evaluar el tipo de incidente presentado, y cuál es el alcance del mismo para posteriormente realizar los procesos de acuerdo a las siguientes incógnitas:

- **¿Incidente conocido?**

✓ Si la respuesta es **SI**, se aplica el método de solución conocido, el cual debe estar documentado y almacenado en la base de conocimiento del CSIRT-UNL.

✓ Si la respuesta es **NO**, el CSIRT-UNL realiza una evaluación más detallada del incidente para aplicar nuevos métodos de solución, los cuales deben ser documentados y almacenados en la base de conocimiento del CSIRT-UNL una vez sea verificado la efectividad de los mismos.

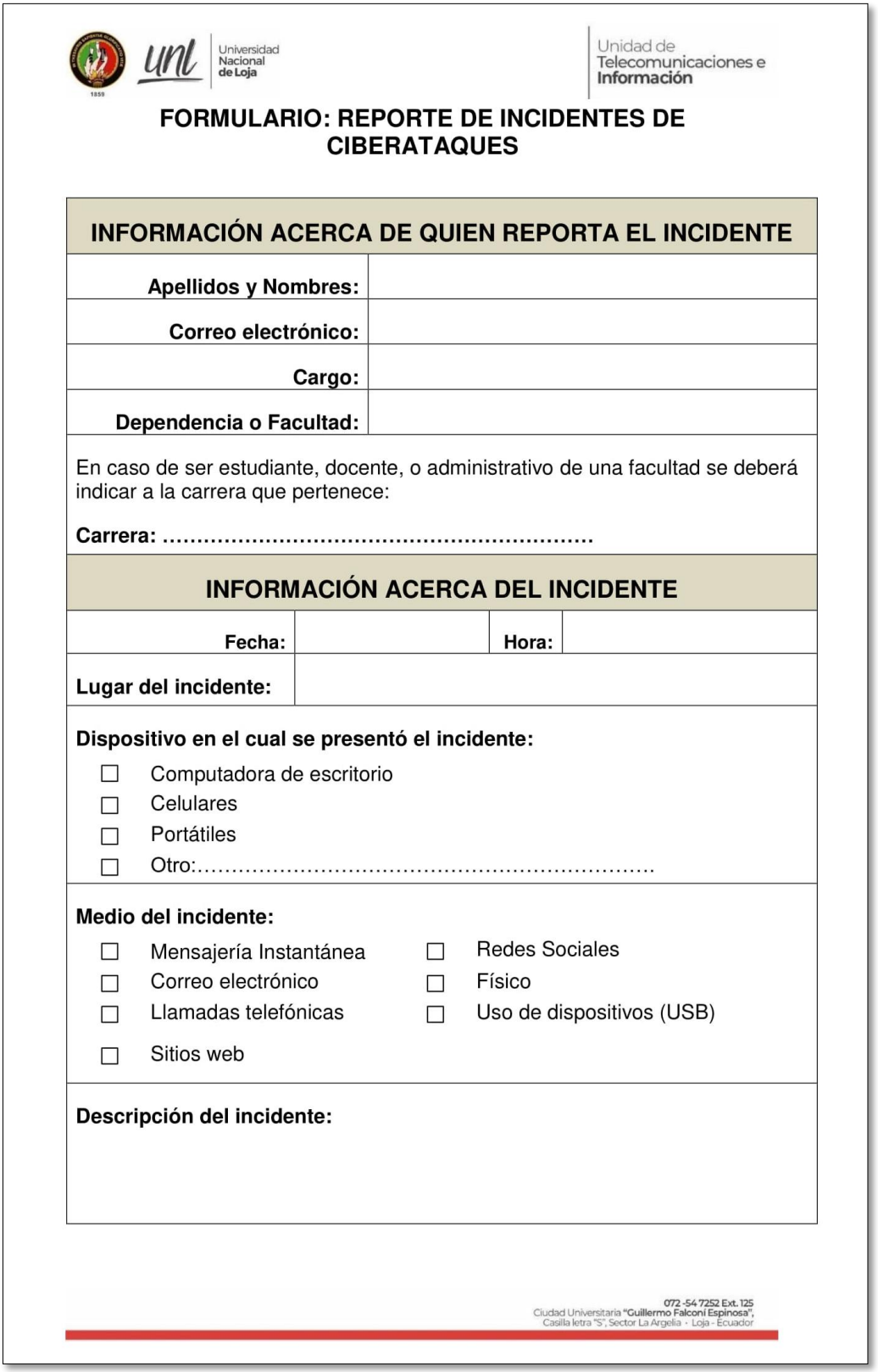
- **¿Incidente solucionado?**

✓ Si la respuesta es **SI**, se reporta al usuario.

✓ Si la respuesta es **NO**, el incidente presentado escalara a una entidad externa (CEDIA, EcuCERT) para ser tratado de acuerdo a sus mecanismos de análisis y solución de incidentes.

También se puede reportar un incidente de seguridad llamando al **072-547252** ext. **125**, o enviando un correo a la cuenta csirt@unl.edu.ec desde su correo institucional.

9. FORMATO PARA REPORTE DE INCIDENTES



Universidad Nacional de Loja

Unidad de Telecomunicaciones e Información

FORMULARIO: REPORTE DE INCIDENTES DE CIBERATAQUES

INFORMACIÓN ACERCA DE QUIEN REPORTA EL INCIDENTE	
Apellidos y Nombres:	
Correo electrónico:	
Cargo:	
Dependencia o Facultad:	

En caso de ser estudiante, docente, o administrativo de una facultad se deberá indicar a la carrera que pertenece:

Carrera: .....

INFORMACIÓN ACERCA DEL INCIDENTE			
Fecha:		**Hora:**	
Lugar del incidente:			

Dispositivo en el cual se presentó el incidente:

- ☐ Computadora de escritorio
- ☐ Celulares
- ☐ Portátiles
- ☐ Otro:.....

Medio del incidente:

- ☐ Mensajería Instantánea
- ☐ Correo electrónico
- ☐ Llamadas telefónicas
- ☐ Sitios web
- ☐ Redes Sociales
- ☐ Físico
- ☐ Uso de dispositivos (USB)

Descripción del incidente:

072-54 7252 Ext. 125
Ciudad Universitaria "Guillermo Falconí Espinosa", Casilla letra "S", Sector La Argelia - Loja - Ecuador

FIGURA 37: *Formato para reporte de incidentes*

FASE 4: Documentar el plan piloto y elaborar el material necesario de concientización para mitigar los ciberataques bajo la modalidad de ingeniería social.

En este objetivo se elaboró el documento formal del plan piloto (ver documento adjunto) y se realizó su presentación a los miembros de la Unidad de Telecomunicaciones e Información UTI con la finalidad de evaluar el cumplimiento de la estructura propuesta en la sección 5 de Materiales y Métodos.

6.4.1. Presentar un borrador del plan piloto.

La presentación del borrador del plan piloto se llevó a cabo el día jueves 15 de agosto del 2019, en la sala de reuniones de la Unidad de Telecomunicaciones e Información UTI (ver ANEXO 7), en presencia de:

- El director de UTI, el Sr. Ingeniero Jhon Calderón Sanmartín.
- El Subdirector de Redes, el Sr. Ingeniero Juan Pablo Ramón.
- El Subdirector de Desarrollo de Software, el Sr. Ingeniero Danny Muñoz.
- El Analista de Sistemas I, el Sr. Máximo Andrés Álvarez Pacheco
- El Tutor Técnico, el Sr. Ingeniero Juan Carlos Riofrío.
- La Tutora Académica, la Srta. Ing. Valeria Herrera Salazar.

Las personas antes mencionadas fueron las encargadas de calificar el cumplimento de la estructura propuesta para el plan piloto mediante la rúbrica presentada en el ANEXO 8.

6.4.2. Revisar y corregir el plan piloto para la entrega de su versión final.

Se procedió con la revisión y corrección del plan piloto en base a las sugerencias y observaciones realizadas por quienes participaron en la presentación del borrador de este, con el fin de dar cumplimiento al objetivo 3 del presente TT.

Como resultado de esto se realizó la entrega del plan piloto para mitigar ciberataques bajo la modalidad de Ingeniería Social al Director de la Unidad de Telecomunicaciones e Información UTI, el 11 de septiembre del 2019. Y posterior se emitió un certificado de finalización del TT con fecha del 27 de Septiembre del 2019 (ver ANEXO 9).

6.4.3. Elaborar el material de concientización entorno a la ingeniería social para la Unidad de Telecomunicaciones e Información de la institución.

El material de concientización entorno a la ingeniería social elaborado es el siguiente:

6.4.3.1. PÁGINA INFORMATIVA:

FIGURA 38: Página Informativa

6.4.3.2. GIGANTOGRAFIAS

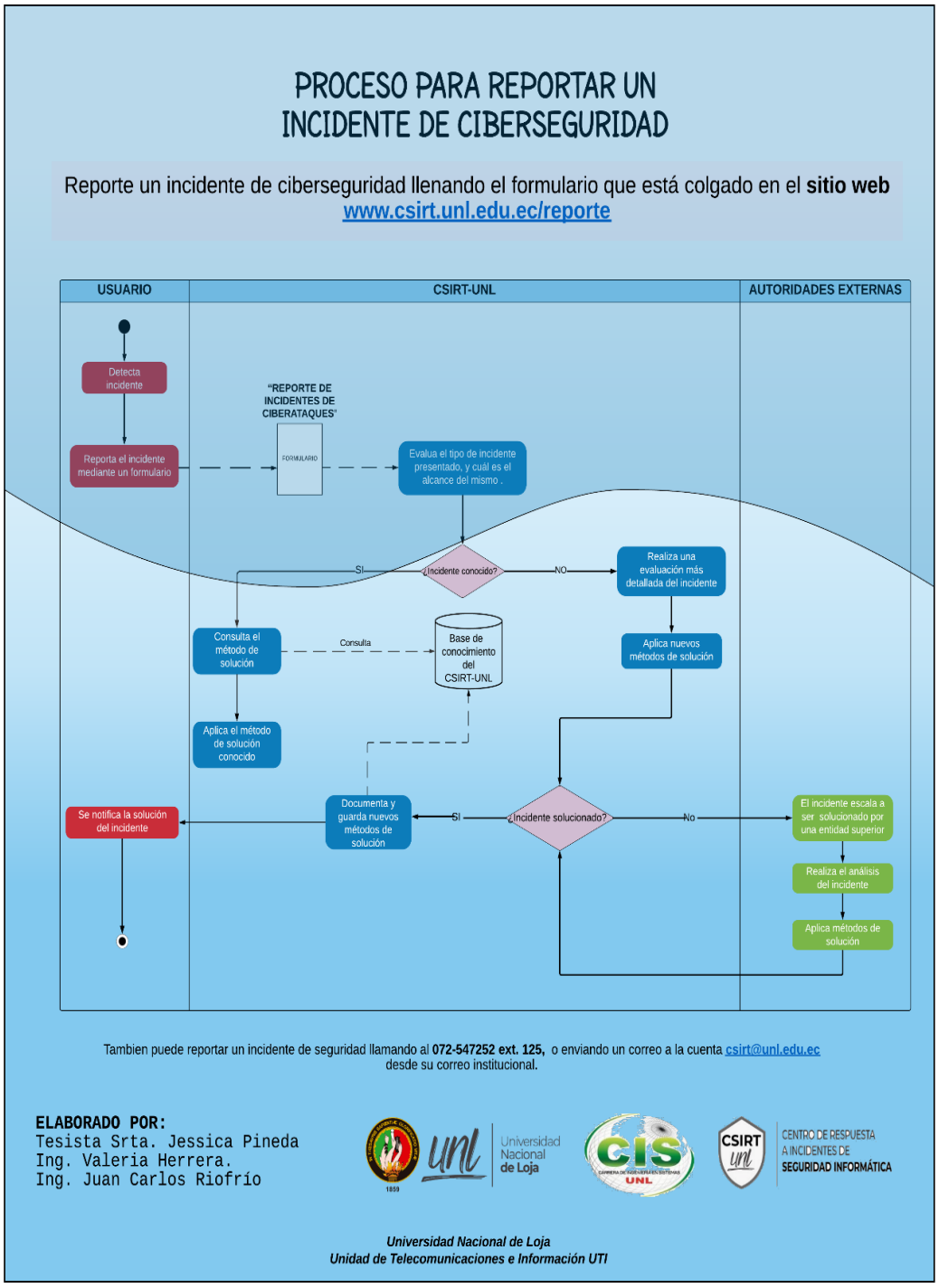


FIGURA 39: *Proceso para reportar un incidente de ciberseguridad*

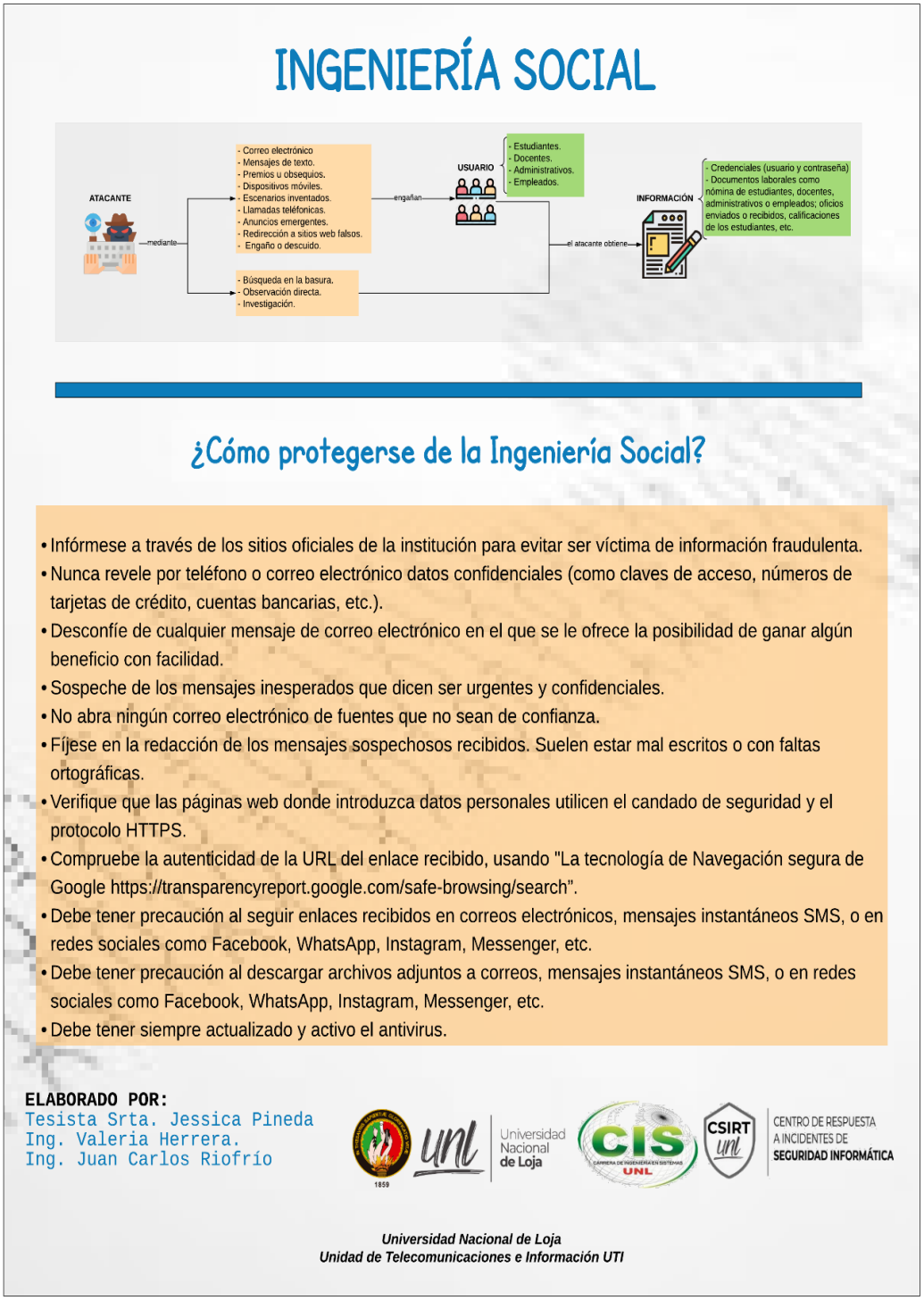


FIGURA 40: *Ingeniería Social*

6.4.3.3. TRIPTICO

FIGURA 41*: Tríptico referente a la Ingeniería Social – Parte 1*

Amenazas de Ingeniería Social

Phishing>>>
Busca engañar a usuario a través del envío de correos electrónicos fraudulentos, con el objetivo de influir u obtener información personal.

Baiting>>>
El atacante deja un dispositivo infectado, como una unidad USB, un teléfono celular o una tarjeta de memoria en algún lugar a propósito, donde personas escogidas específicamente puedan encontrarlo e infectar sus computadores.

Smishing>>>
El atacante usa mensajes de teléfono móvil (SMS) para lograr que las víctimas tomen acciones inmediatas con el objetivo de influir u obtener información personal.

Quid Pro Quo>>>
El atacante promete algún beneficio a la víctima a cambio de información sensible de la organización o del mismo usuario.

Pretexting>>>
El atacante crea un escenario inventado para engañar al usuario, con el objetivo de robar información importante y sensible a la víctima.

Pharming>>>
El atacante se infiltra en un sistema informático e instala un código malicioso que hace que el tráfico del sitio web del sistema se redirija a sitios falsos desarrollados por el pirata informático.

Vishing>>>
El atacante realiza llamadas telefónicas suplantando a compañías de servicios o de gobierno mediante las cuales se busca engañar a la víctima para que revele información privada.

Spear - Phishing>>>
El atacante utiliza el correo electrónico o comunicaciones electrónicas para engañar a personas concretas u organizaciones específicas.

Dumpster Diving>>>
El atacante utiliza el correo electrónico o comunicaciones electrónicas para engañar a personas concretas u organizaciones específicas.

Shoulder Surfing>>>
El atacante recopila información personal o privada a través de la observación directa en una pantalla por estar físicamente cerca de ella y tener acceso a la lectura de la información digitada por la víctima.

Espionaje Industrial>>>
El atacante consigue introducirse en los sistemas informáticos de la empresa y robar información valiosa para obtener una ventaja comercial.

Tailgating>>>
El atacante obtiene el acceso a las áreas restringidas como oficinas o centros de datos, mediante el engaño o descuido de una persona con la autorización correspondiente.

Scareware>>>
Es una táctica de malware que manipula a los usuarios para que descarguen, instalen o compren software malintencionado que exponga datos confidenciales.

FIGURA 42: *Tríptico referente a la Ingeniería Social – Parte 2*

6.4.3.4. COMUNICADO

FIGURA 43: *Comunicado para informar a la comunidad Universitaria*

7. Discusión

En este apartado se muestra el desarrollo de la propuesta alternativa, en donde se interpreta los resultados obtenidos del cumplimiento de cada objetivo del presente TT, los mismos que fueron propuestos considerando que existe un desconocimiento de los ciberataques bajo la modalidad de Ingeniería Social en la Universidad Nacional de Loja; además se realiza la valoración económica del presente trabajo.

7.1. Desarrollo de la Propuesta Alternativa

OBJETIVO 1. Revisión bibliográfica entorno a la ingeniería social.

Para la discusión del primer objetivo se procedió a contestar las 2 preguntas de investigación definidas en la Revisión Sistemática de Literatura.

a) Técnicas de ataque bajo la modalidad de Ingeniería Social.

Con la evaluación de calidad realizada a los artículos seleccionados en la SRL se pudo identificar las técnicas de ataque en cada uno de ellos, la cuales están detalladas en la TABLA 6. Según los datos mostrados en esta tabla se obtuvo que la técnica más relevante es el Phishing, seguido del Baiting, Pretexting, Pharming, Vhishing, Tailgating, y el Quid Pro Quo; y las técnicas menos sobresalientes son: Smishing, Spear-Phishing, Dumpster Diving, Shoulder Surfing, Espionaje Industrial, y el Shareware.

b) Métodos para mitigar ataques bajo la modalidad de Ingeniería Social.

Los métodos (salvaguardias) para mitigar un ataque de Ingeniería Social reconocidos en cada artículo son parte del detalle de la TABLA 6, en base a esta tabla se obtuvo que la salvaguardia más usada es la Educación - Capacitación y Concientización, la misma que fue identificada en la mayoría de los artículos excepto en el AR05, AR08, AR16, AR19, AR20, AR21, AR24, AR25, AR27 Y AR28. Otras salvaguardias relevantes son las técnicas de seguridad lógica y las políticas.

OBJETIVO 2. Simular un ciberataque bajo la modalidad de Ingeniería Social.

Este objetivo se planteó para demostrar que el usuario desconoce acerca de los ciberataques bajo la modalidad de Ingeniería Social y por lo tanto es vulnerable a los mismos; para esto se delimitó la población a la cual se enfocaría el cumplimiento de este objetivo, se realizó el proceso de Análisis de Riesgos, y se aplicó la encuesta (ver ANEXO 5).

De acuerdo a los resultados del proceso de análisis de riesgos se puede decir que el phishing es una de las amenazas más comunes y con un alto riesgo de probabilidad de ocurrencia e impacto para la institución, lo cual comprueba lo mencionado en los artículos [6][42][20][45][59][60]. En base a lo expuesto se determinó que está amenaza sería utilizada en la simulación.

A través de los resultados de la encuesta aplicada se determinó que el correo electrónico sería el medio usado para realizar la simulación. Además se demostró que el usuario desconoce de los ciberataques bajo la modalidad de Ingeniería social, lo cual lo convierte en un activo vulnerable a esta modalidad; con esto se corrobora que “el usuario es el eslabón más débil de una empresa o institución”, mencionado en los artículos [6][7][20][15][45].

Finalmente, los resultados obtenidos en la simulación corroboran que la técnica de phishing es efectiva para hacer que el usuario sea vulnerable a ciberataques de Ingeniería Social.

OBJETIVO 3. Desarrollar el plan piloto para mitigar los ciberataques bajo la modalidad de ingeniería social.

Con este objetivo se buscó dar cumplimiento al propósito principal del presente TT, para lo cual se cumplió con el siguiente esquema: 1) LIMITACIONES A LA DIVULGACIÓN DEL USO DEL INFORME en donde se determinó a quien va dirigido el plan piloto; 2) ANTECEDENTES hace referencia a la base legal en la cual se sustenta el plan piloto; 3) ALCANCE; 4) OBJETIVO en donde se describió el propósito para el cual fue creado el plan piloto; 5) JUSTIFICACIÓN en donde se expuso las razones por las cuales se realiza el plan piloto; 6) DEFINICIONES en donde constan los términos asociados al desarrollo del plan piloto, evitando ambigüedades en los términos usados y permitiendo dar al lector una mayor claridad del tema; 7) ANÁLISIS DEL RIESGO, fue el proceso que permitió establecer salvaguardias que mitiguen la materialización de las amenazas bajo la modalidad de Ingeniería Social identificadas (ver TABLA 5). Las salvaguardias fueron establecidas tomando en cuenta los resultados de la SRL (ver TABLA 6) y en base a la estructura de la ISO 27002:2013 (ver FIGURA 2); 8) PROCESO DE ATENCIÓN A INCIDENTES, sección en la cual se propuso los pasos a seguir para que la comunidad universitaria reporte un incidente de Ciberseguridad; 9) FORMATO PARA REPORTE DE INCIDENTES

OBJETIVO 4. Revisar y corregir el plan piloto para la entrega de su versión final.

El propósito de este objetivo es realizar la revisión y correcciones necesarias para hacer la entrega formal a la UTI de la versión final del plan piloto para mitigar ciberataques bajo la modalidad de Ingeniería Social y del material de capacitación y concientización. Para dar cumplimiento a este objetivo se realizó la exposición del plan piloto y la valoración del cumplimiento de las secciones que conforman el mismo, además se realizó el control de asistencia (ver ANEXO 7). En base a las observaciones presentadas por quienes acudieron a la exposición se realizaron las correcciones necesarias para obtener la versión final del plan piloto y realizar su entrega.

7.2. Valoración técnica económica ambiental

La inversión económica que conllevo dar cumplimiento a los objetivos planteados para el desarrollo del presente TT, se detallan en la TABLA 28:

TABLA 28: *Valoración económica del TT.*

RECURSO HUMANO			
Equipo de trabajo	**Horas**	**Precio/Hora**	**Valor Total**
Tesista	780	$10,00	$7.800,00
Director	81	$15,00	$1.215,00
SUBTOTAL			**$9.015,00**
RECURSO HARDWARE			
Descripción	**Cantidad**	**Valor**	**Valor Total**
Computadora	1	$00,00	$00,00
Impresora	1	$00,00	$00,00
USB	1	$00,00	$00,00
SUBTOTAL			$00,00

RECURSO SOFTWARE			
Descripción	**Cantidad**	**Valor**	**Valor Total**
Kali linux	1	$0,00	$0,00
Google drive	1	$0,00	$0,00
Mendeley Desktop	1	$0,00	$0,00
Procesador de texto	1	$0,00	$0,00
Social engineering toolkit	1	$0,00	$0,00
Google Analytics	1	$0,00	$0,00
LucidChart	1	$0,00	$0,00
Parsifal	1	$0,00	$0,00
SUBTOTAL			**$0,00**
RECURSO VARIOS			
Descripción	**Cantidad**	**Valor**	**Valor Total**
Internet	480 Hr	$0,60	$288,00
Impresiones B/N	230	$0,05	$11,50
Impresiones color	133	$0,10	$13,30
SUBTOTAL			**$312,80**
TOTAL			**$9327,80**

Debido a que los recursos usados en este TT son software libre y Open Source tienen una valoración de cero dólares.

8. CONCLUSIONES

En base a los resultados obtenidos del cumplimiento de los objetivos propuestos para el presente trabajo, se concluye lo siguiente:

- ✓ Mediante la SRL realizada se reconoció que las técnicas de Ingeniería social más relevantes son el phishing, baiting, y el quid pro quo; así mismo se identificó que las salvaguardias más sobresalientes son la educación - capacitación y concientización, las técnicas de seguridad lógica, y las políticas.
- ✓ La SRL además permitió conocer que las empresas tienden a establecer salvaguardias principalmente para el cuidado de los activos de hardware y software, ignorando al usuario que hace uso de estos, motivo por el cual se convierte en un activo vulnerable para ser víctima a ciberataques bajo la modalidad de Ingeniería Social. Así mismo la falta de capacitación y concientización al usuario, hacen de este un activo vulnerable a realizar acciones que comprometan la integridad, confidencialidad, y disponibilidad de la información de la institución.
- ✓ Con la valoración del riesgo realizada a las 13 amenazas de Ingeniería Social, se puede mencionar que las 2 amenazas con mayor riesgo para comprometer al usuario y a la información son el tailgating que se encuentra en un nivel de riesgo crítico, y el phishing que está en un nivel de riesgo alto; mientras que las amenazas restantes se encuentran en un riesgo moderado o bajo, esto de acuerdo a las escalas establecidas para los niveles de riesgo.
- ✓ Como consecuencia del análisis de la encuesta aplicada se puede afirmar que los usuarios de la comunidad universitaria además de hacer uso del internet para sus obligaciones laborales lo utilizan para actividades ajenas al trabajo como: descarga de archivos, ingreso a redes sociales, y para entretenimiento (descargar/escuchar música, ver videos/películas, jugar, etc); lo cual pone en riesgo su integridad personal y la de la institución.
- ✓ Asimismo, la falta de conocimiento de los usuarios acerca de la Ingeniería Social podría conllevar a la materialización de un delito informático en el cual se vea comprometido al menos uno de los principios de la seguridad de la información, perjudicando al usuario o a la institución en sí; en este sentido los usuarios no deben desconocer las leyes que penalizan un delito de esta índole.

- ✓ El éxito de la simulación realizada esta representado por el 84,65% del total de ataques enviados a la población delimitada, lo cual indica que los usuarios son vulnerables a ciberataques bajo la modalidad de ingeniería social; esto debido a que la página web de la institución revela información útil para ejecutar un ciberataque, además de que los usuarios desconocen de los peligros a los cuales están expuestos al navegar en internet o por el desconocimiento para identificar un correo electrónico falso.
- ✓ Finalmente, con el cumplimento del Plan Piloto y del material de concientización entregado se da paso a que este trabajo pueda ser implementado por La Unidad de Telecomunicaciones e Información UTI. Cabe mencionar que la implementación no forma parte del alcance del presente TT, quedando a desarrollarse como un trabajo futuro.

9. RECOMENDACIONES

Una vez concluido el presente TT se recomienda lo siguiente:

A la Unidad de Telecomunicaciones e Información UTI,

- ✓ Con el apoyo de las carreras afines a la tecnología, realizar al menos dos talleres al año para capacitar y concientizar a la comunidad universitaria acerca de los peligros a los cuales se encuentran expuestos al navegar en internet.
- ✓ De acuerdo con el rol del usuario y a la información que tenga acceso, implementar políticas y mecanismos para restringir el acceso a sitios web ajenos a las actividades que desempeñan.
- ✓ Con el apoyo del departamento de comunicación, y del correo institucional mantener informada a toda la comunidad universitaria acerca de los tipos de delitos informáticos existentes y sobre la ley que los penaliza; así mismo se debe informar sobre casos de incidentes de Ciberseguridad suscitados con la finalidad de crear conciencia en el usuario.

A la comunidad universitaria,

- ✓ Tomar en cuenta las buenas prácticas expuestas por UTI para el uso correcto del correo electrónico institucional.
- ✓ Mantenerse Informado acerca del marco legal que respalda el buen uso de la información con la finalidad de salvaguardar la integridad de los datos.
- ✓ Comunicar de forma inmediata a quien corresponda el suceso de un incidente de Ciberseguridad.

10. BIBLIOGRAFÍA

[1] L. Xd, “Propuesta metodológica para la evaluación de seguridad de usuarios de redes sociales con relación a ataques de ingeniería social,” 2017.

[2] J. Domínguez Chávez, “Aspectos interesantes sobre la Ingeniería Social,” *www.researchgate.net, Univ. Politécnica Territ. del estado Aragua “Federico Brito Figueroa,”* p. 7, 2014.

[3] A. Correa Sierra, C. A. Orrego Ossa, I. de Sistemas, corea000@hotmail.com, and corrego@eafit.edu.co, “The Social Engineering framework para el aseguramiento de PYME,” 2015.

[4] I. E. A. N. GUTIERREZ, “INGENIERÍA SOCIAL COMO DELITO INFORMÁTICO EN LAS GRANDES EMPRESAS COLOMBIANAS,” UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD FACULTAD, 2018.

[5] H. Wilcox and M. Bhattacharya, “A Framework to Mitigate Social Engineering through Social Media within the Enterprise.” IEEE, p. 6, 2016.

[6] C. E. L. Grande and R. S. Guadrón, “Social Engineering : The Silent Attack,” no. Concapan Xxxv, 2015.

[7] A. Cullen and L. Armitage, “The Social Engineering Attack Spiral (SEAS).”

[8] I. Ghafir, “Social Engineering Attack Strategies and Defence Approaches,” 2016.

[9] Z. L. Švehla, I. Sedinić, and L. Pauk, “Going White Hat : Security Check by Hacking Employees Using Social Engineering Techniques,” pp. 1419–1422, 2016.

[10] F. Mouton, L. Leenen, and H. S. Venter, “Social engineering attack examples, Templates and Scenarios,” *Comput. Secur.*, vol. 59, pp. 186–209, 2016.

[11] K. Y. Abeywardana, E. Pfluegel, and M. J. Tunnicliffe, “A layered defense mechanism for a social engineering aware perimeter,” *Proc. 2016 SAI Comput. Conf. SAI 2016*, pp. 1054–1062, 2016.

[12] J. Andrés and V. Rodríguez, “Ingeniería Social . La práctica de obtener información confidencial Social engineering . Practice of confidential information obtained,” no. 3, 2017.

[13] BBC Mundo Tencología, “Qué es el "smishing" y cómo puedes detectarlo en tu celular para que no te estafen,” *2 agosto* , 2017. [Online].

Available: https://www.bbc.com/mundo/noticias-40802167. [Accessed: 27-Aug-2019].

[14] Meritxell Oncins Domènech, “Hablemos de ciberseguridad – VI – Smishing (phishing via SMS),” *8 agosto*, 2017. [Online]. Available: https://www.iniseg.es/blog/ciberseguridad/hablemos-de-ciberseguridad-vi-smishing-phishing-via-sms/. [Accessed: 27-Aug-2019].

[15] A. S. Alazri, “The awareness of social engineering in information revolution: Techniques and challenges,” *2015 10th Int. Conf. Internet Technol. Secur. Trans. ICITST 2015*, pp. 198–201, 2016.

[16] Lyna Griffin, “What is a Pharming Attack? - Definition & Examples | Study.com,” 2017. [Online]. Available: https://study.com/academy/lesson/what-is-a-pharming-attack-definition-examples.html. [Accessed: 27-Aug-2019].

[17] Panda, “Pharming Overview and Defense Tactics - Panda Security Mediacenter,” *April 18* , 2019. [Online]. Available: https://www.pandasecurity.com/mediacenter/panda-security/pharming/. [Accessed: 27-Aug-2019].

[18] “Generating pharming alerts with reduced false positives,” 2017.

[19] H. Wilcox and M. Bhattacharya, “Countering social engineering through social media: An enterprise security perspective,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9330 LNCS, pp. 54–64, 2015.

[20] T. Bakhshi, “Social engineering: Revisiting end-user awareness and susceptibility to classic attack vectors,” *Proc. - 2017 13th Int. Conf. Emerg. Technol. ICET2017*, vol. 2018-Janua, pp. 1–6, 2018.

[21] Sociedad Andaluza para el Desarrollo de las Telecomunicaciones S.A, “Informe de divulgación Phishing,” 2017.

[22] M. Sheila, M. Leguizamón, and M. M. Villanueva, “EL PHISHING TRABAJO FINAL DE GRADO. GRADO EN CRIMINOLOGÍA Y SEGURIDAD.”

[23] M. Castro, “INGENIERIA SOCIAL, EL ELEMENTO HUMANO DE LA SEGURIDAD; CONTRAMEDIDAS Y PLANES DE ACCION PARA FORTALECER LA SEGURIDAD EN LAS ORGANIZACIONES.,” 2016.

[24] incibe-cert_, “Información privilegiada y ciberespionaje industrial,” *25 de Octubre*, 2018. [Online]. Available: https://www.incibe-cert.es/blog/informacion-

privilegiada-y-ciberespionaje-industrial. [Accessed: 27-Aug-2019].

[25] C. D. S. JORGE MARCOS, “Ciberseguridad en el espionaje industrial,” 2018. [Online]. Available: http://www.redseguridad.com/sectores-tic/industria-y-utilities/ciberseguridad-en-el-espionaje-industrial. [Accessed: 27-Aug-2019].

[26] O. Alejandro, T. Diaz, D. Juan, and P. L. Rodriguez, “DISEÑO E IMPLEMENTACIÓN DE UN PLAN DE CONCIENTIZACIÓN FRENTE A LA INGENIERÍA SOCIAL PARA LA EMPRESA PROMOCIONES Y COBRANZAS BETA S.A.,” UNIVERSIDAD PILOTO DE COLOMBIA, 2017.

[27] E. Piscitelli, “El verdadero poder de la ingeniería social,” *USERS 317. Android*, p. 10, 2017.

[28] Panda Security, “Scareware: info sobre este software malicioso,” 2019. [Online]. Available: https://www.pandasecurity.com/es/security-info/scareware/. [Accessed: 27-Aug-2019].

[29] “La Ingeniería Social: El Arte del Engaño,” 2015.

[30] O. Olivos, “Creating a Security Culture Development Plan and a Case Study,” *Proceeding Sixt Symp. Hum. Asp. Inf. Secur. Asssurance*, no. Haisa, pp. 13–32, 2012.

[31] C. Ing. Enrique Larrieu-Let, “Ciberataques ¿Estamos preparados?” 2015.

[32] DR. SANTIAGO ACURIO DEL PINO, “Delitos Informáticos: Generalidades,” 2016.

[33] A. J. E. Zambrano-mendieta, A. K. I. Dueñas-zambrano, and A. L. M. Macías-ordoñez, “Delito Informático . Procedimiento Penal en Ecuador,” vol. 2. pp. 204–215, 2016.

[34] Ricardo Antonio Parada ; José Daniel Errecaborde, “CIBERCRIMEN Y DELITOS INFORMÁTICOS,” vol. 1a ed, p. 196, 2018.

[35] I. Maurice, “Taller de Implementación de la norma ISO 27001,” Perú, 2018.

[36] ISO 27001, “ISO 27000 - Glosario de términos.” .

[37] Ing. Wáshington Marcelo Contero Ramos, “DISEÑO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN BASADA EN LA NORMA ISO 27002:2013, PARA EL SISTEMA DE BOTONES DE SEGURIDAD DEL MINISTERIO DEL INTERIOR.” p. 123, 2019.

[38] Tapia J, “ISO 27002:2013,” *GES|CONSULTOR*. p. 1, 2013.

[39] R. O. S. De, L. F. Badillo, and R. Oficial, “LEY ORGANICA DEL SISTEMA

NACIONAL DE REGISTRO DE DATOS PUBLICOS," pp. 1–15, 2017.

[40] S. A. D. T. P. Kaushalya, R. M. R. S. B. Randeniya, and A. D. S. Liyanage, "An Overview of Social Engineering in the Context of Information Security," *2018 IEEE 5th Int. Conf. Eng. Technol. Appl. Sci. ICETAS 2018*, pp. 1–6, 2019.

[41] B. B. Gupta, N. A. G. Arachchilage, and K. E. Psannis, "Defending against phishing attacks: taxonomy of methods, current issues and future directions," *Telecommun. Syst.*, vol. 67, no. 2, pp. 247–267, 2018.

[42] S. Gupta, A. Singhal, and A. Kapoor, "A literature survey on social engineering attacks: Phishing attack," *Proceeding - IEEE Int. Conf. Comput. Commun. Autom. ICCCA 2016*, pp. 537–540, 2017.

[43] R. McEvoy and S. Kowalski, "Beyond training and awareness: From security culture to security risk management," *CEUR Workshop Proc.*, vol. 2107, pp. 71–86, 2018.

[44] M. Silic and A. Back, "The dark side of social networking sites:Understanding phishing risks," *Comput. Human Behav.*, vol. 60, pp. 35–43, 2016.

[45] I. E. Van Vuuren, E. Kritzinger, and C. Mueller, "Identifying gaps in IT retail Information Security policy implementation processes," *2015 2nd Int. Conf. Inf. Secur. Cyber Forensics, InfoSec 2015*, pp. 126–133, 2016.

[46] C. C. Campbell, "Solutions for counteracting human deception in social engineering attacks," *Inf. Technol. People*, 2018.

[47] D. Choi, C. Choi, and X. Su, "Invisible secure keypad solution resilient against shoulder surfing attacks," *Proc. - 2016 10th Int. Conf. Innov. Mob. Internet Serv. Ubiquitous Comput. IMIS 2016*, pp. 514–517, 2016.

[48] P. L. Gallegos-Segovia, P. E. Vintimilla-Tapia, J. F. Bravo-Torres, I. F. Yuquilima-Albarado, V. M. Larios-Rosillo, and J. D. Jara-Saltos, "Social engineering as an attack vector for ransomware," *2017 Chil. Conf. Electr. Electron. Eng. Inf. Commun. Technol. CHILECON 2017 - Proc.*, vol. 2017-Janua, pp. 1–6, 2017.

[49] A. Anir Norman, M. Maw Hanifa, S. Hamid, and S. I. Ramrin, "Security Threats and Techniques in Social Networking Sites: A Systematic Literature Review," *Futur. Technol. Conf.*, vol. November, no. Vancouver, Canada, p. 20, 2017.

[50] B. Arya and K. Chandrasekaran, "A client-side anti-pharming (CSAP) approach," *Proc. IEEE Int. Conf. Circuit, Power Comput. Technol. ICCPCT 2016*, 2016.

[51] R. Bhakta and I. G. Harris, "Semantic analysis of dialogs to detect social

engineering attacks," *Proc. 2015 IEEE 9th Int. Conf. Semant. Comput. IEEE ICSC 2015*, pp. 424–427, 2015.

[52] J. D. Ndibwile, Y. Kadobayashi, and D. Fall, "UnPhishMe: Phishing Attack Detection by Deceptive Login Simulation through an Android Mobile App," *Proc. - 12th Asia Jt. Conf. Inf. Secur. AsiaJCIS 2017*, pp. 38–47, 2017.

[53] Ş. Şentürk, E. Yerli, and İ. Soğukpnar, "Email phishing detection and prevention by using data mining techniques," *2nd Int. Conf. Comput. Sci. Eng. UBMK 2017*, pp. 707–712, 2017.

[54] A. Aleroud and L. Zhou, "Phishing environments, techniques, and countermeasures: A survey," *Comput. Secur.*, vol. 68, no. April, pp. 160–196, 2017.

[55] A. N. Shaikh, A. M. Shabut, and M. A. Hossain, "A literature review on phishing crime, prevention review and investigation of gaps," *Ski. 2016 - 2016 10th Int. Conf. Software, Knowledge, Inf. Manag. Appl.*, pp. 9–15, 2017.

[56] S. Al-Sharif, F. Iqbal, T. Baker, and A. Khattack, "White-hat hacking framework for promoting security awareness," *2016 8th IFIP Int. Conf. New Technol. Mobil. Secur. NTMS 2016*, 2016.

[57] T. Bhardwaj, T. K. Sharma, and M. R. Pandit, "Social engineering prevention by detecting malicious URLs using artificial bee colony algorithm," *Adv. Intell. Syst. Comput.*, vol. 258, no. January, pp. 355–363, 2014.

[58] "About · Parsifal." [Online]. Available: https://parsif.al/about/. [Accessed: 08-Jan-2020].

[59] J. Rastenis, S. Ramanauskaite, J. Janulevicius, and A. Cenys, "Credulity to Phishing Attacks: A Real-World Study of Personnel with Higher Education," *2019 Open Conf. Electr. Electron. Inf. Sci. eStream 2019 - Proc.*, pp. 1–5, 2019.

[60] A. A. Andryukhin, "Phishing Attacks and Preventions in Blockchain Based Projects," *Proc. - 2019 Int. Conf. Eng. Technol. Comput. Sci. Innov. Appl. EnT 2019*, pp. 15–19, 2019.

11. ANEXOS

Anexo 1: Código Orgánico Integral Penal COIP.

a) Artículos para penalizar un delito de Ingeniería Social

- **Artículo 178.- Violación a la intimidad. -** "La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años. (..)"

- **Artículo 179.- Revelación de secreto. -** La persona que, teniendo conocimiento por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año.

- **Artículo 180.- Difusión de información de circulación restringida. -** "La persona que difunda información de circulación restringida será sancionada con pena privativa de libertad de uno a tres años (…)."

- **Artículo 181.- Violación de propiedad privada. -** "La persona que, con engaños o de manera clandestina, ingrese o se mantenga en morada, casa, negocio, dependencia o recinto habitado por otra, en contra de la voluntad expresa o presunta de quien tenga derecho a excluirla, será sancionada con pena privativa de libertad de seis meses a un año. (…) "

- **Artículo 186.- Estafa. - "**La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años.

La pena máxima se aplicará a la persona que:

1. Defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario.
2. Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares.
3. Entregue certificación falsa sobre las operaciones o inversiones que realice la persona jurídica.
4. Induzca a la compra o venta pública de valores por medio de cualquier acto, práctica, mecanismo o artificio engañoso o fraudulento.
5. Efectúe cotizaciones o transacciones ficticias respecto de cualquier valor. (…)"

- **Artículo 190.- Apropiación fraudulenta por medios electrónicos.-** "La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.

  La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes."

- **Artículo 212.- Suplantación de identidad. -** "La persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una persona, será sancionada con pena privativa de libertad de uno a tres años."

- **Artículo 229.- Revelación ilegal de base de datos. -** "La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. (…)"

- **Artículo 230.- Interceptación ilegal de datos. -** "Será sancionada con pena privativa de libertad de tres a cinco años:

  1. La persona que, sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.
  2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.
  3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.
  4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior. "

- **Artículo 231.- Transferencia electrónica de activo patrimonial. -** "La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona

en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.

- **Artículo 232.- Ataque a la integridad de sistemas informáticos. -** "La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.

  Con igual pena será sancionada la persona que:

  1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.
  2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

     Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad."

- **Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.-** "La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos

sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años."

- **Artículo 235.- Engaño al comprador respecto a la identidad o calidad de las cosas o servicios vendidos.-** "La persona que provoque error al comprador o al usuario acerca de la identidad o calidad de la cosa o servicio vendido, entregando fraudulentamente un distinto objeto o servicio ofertado en la publicidad, información o contrato o acerca de la naturaleza u origen de la cosa o servicio vendido, entregando una semejante en apariencia a la que se ha comprado o creído comprar, será sancionada con pena privativa de libertad de seis meses a un año. (…)"

- **Artículo 351.- Infiltración en zonas de seguridad. -** La persona que se introduzca injustificadamente en zonas de seguridad, cuyo acceso al público ha sido prohibido, será sancionada con pena privativa de libertad de seis meses a dos años.

b) Validación del análisis - COIP.

Loja, 21 de Julio del 2020

A quien corresponda.

Por medio del presente, a petición verbal de la interesada, me permito validar el análisis realizado en base a la normativa del Código Orgánico Integral Penal COIP, donde se faculta la penalización de conductas delictivas derivadas de la Ingeniería Social, citados en la TABLA 1 del Trabajo de Titulación denominado **"Plan piloto para la mitigación de ciberataques bajo la modalidad de Ingeniería Social en la Universidad Nacional de Loja".**

Atentamente,

Abg. Viviana Torres Montaño
Mtro. Nro. 11-2020-187

ABG. VIVIANA TORRES MONTAÑO
MTR. Nº 11-2019-187

Anexo 2: Revisión Sistemática De Literatura SRL

Ingeniería Social: Revisión Sistemática de Literatura

En base a la metodología de revisiones sistemáticas de Kitchenham y Brereton se estableció el protocolo para la revisión, selección y extracción de información acerca del objeto de estudio.

a. Preguntas de investigación.

A partir de la temática central denominada “Ingeniería Social” se planteó cinco preguntas de investigación clasificadas en preguntas para el mapeo sistemático (MQ) y la revisión sistemática (RQ):

- **MQ1:** ¿Cuántos estudios se publicaron a lo largo de los años en el área de ingeniería social?
- **MQ2:** ¿Quiénes son los autores más relevantes y activos en esta área?
- **MQ3:** ¿Cuáles son las revistas y congresos que se han publicado en el área?
- **RQ1:** ¿Cuáles son las técnicas de ataque bajo la modalidad de ingeniería social?
- **RQ2:** ¿Cuáles son los métodos para mitigar ataques bajo la modalidad de ingeniería social?

b. Proceso de búsqueda.

El siguiente paso es determinar el conjunto de términos basados en las preguntas de investigación para construir la cadena de búsqueda. Se utilizó el método Picoc propuesto por Petticrew para definir el ámbito de la SRL:

- **Población** (P): Social engineering, Social engineering attack
- **Intervención** (I): Methods, techniques
- **Comparación** (C): Don not apply
- **Resultados** (O): prevention techniques, prevention, social engineering prevention, *Social engineering attacks.*
- **Contexto** (C): Security information, Social engineering

c. Definición de los criterios de inclusión y exclusión.

Se especificaron 6 criterios de inclusión (IC):

- **IC1**: Los artículos deben estar relacionados con el área de Ingeniería Social AND
- **IC2**: Los artículos deben contener información sobre técnicas OR métodos de ataque bajo la modalidad de ingeniería social, AND
- **IC3**: Los artículos deben contener información sobre técnicas OR métodos de prevención OR salvaguardias AND
- **IC4**: Los artículos deben estar escritos en inglés OR español AND
- **IC5**: Los artículos deben haber sido publicados en congresos OR revistas científicas AND
- **IC6**: Artículos que hayan sido publicados desde el 2014 en adelante.

- Se especificaron 5 criterios de exclusión (EC):
- **EC1**: Artículos que no estén relacionados con la rama de la ingeniería social en las ciencias computacionales OR.
- **EC2**: Los artículos que no posean información sobre métodos OR técnicas de ataque bajo la modalidad de ingeniería social, OR
- **EC3**: Los artículos que hayan sido publicados en capítulos de libro OR workshop OR
- **EC4**: Artículos que hayan sido publicados antes el 2014 OR
- **EC5**: Artículos parciales o investigaciones que se encuentren en desarrollo OR.

d. Definición de las bases de datos.

- IEEEXplore (ieeexplore.ieee.org)
- Scopus (http://www.scopus.com)

e. Cadenas de Búsqueda.

Para crear la cadena de búsqueda se utilizó los términos definidos en las preguntas de investigación, del método Picoc. Se definieron palabras clave como: Ataques de ingeniería social, prevención de la ingeniería social, técnicas de prevención, ingeniería social; que permitieron junto con la sinonimia de cada palabra realizar diversas combinaciones, usando operadores lógicos “OR” para los conceptos similares, “AND” para los conceptos complementarios y “NOT” para los términos excluyentes.

Las búsquedas aplicadas en las bases de datos seleccionadas fueron las siguientes:

Cadena genérica:

("Social engineering" OR "Social engineering attack") AND ("methods" OR "techniques") AND ("prevention" OR "prevention techniques" OR "social engineering prevention")

IEEE Library:

("Social engineering" OR "Social engineering attack") AND ("methods" OR "techniques") AND ("prevention" OR "prevention techniques" OR "social engineering prevention")

Scopus:

TITLE-ABS-KEY (("Social engineering" OR "Social engineering attack") AND ("methods" OR "techniques") AND ("prevention" OR "prevention techniques" OR "social engineering prevention")) AND (EXCLUDE (PUBYEAR , 2013) OR EXCLUDE (PUBYEAR , 2012) OR EXCLUDE (PUBYEAR , 2011) OR EXCLUDE (PUBYEAR , 2010) OR EXCLUDE (PUBYEAR , 2009) OR EXCLUDE (PUBYEAR , 2008) OR EXCLUDE (PUBYEAR , 2007) OR EXCLUDE (PUBYEAR , 2006) OR EXCLUDE (PUBYEAR , 2005) OR EXCLUDE (PUBYEAR , 2004) OR EXCLUDE (PUBYEAR , 1976)) AND (EXCLUDE (SUBJAREA , "BUSI") OR EXCLUDE (SUBJAREA , "ECON")) AND (EXCLUDE (SUBJAREA , "MEDI"))

f. Evaluación de calidad.

Para la evaluación de calidad de cada artículo se establecieron las siguientes preguntas:

- **QA1:** ¿El artículo se enfoca a la seguridad de la información en el contexto de Ingeniería Social?
- **QA2:** ¿Se identifica algún método para mitigar ataques bajo la modalidad de Ingeniería Social?
- **QA3:** ¿El artículo identifica alguna técnica de ataque bajo la modalidad de Ingeniería social?

Cada una de las preguntas planteadas tuvo un puntaje de 1 si se califica con “Si”, 0.5 si la respuesta es “Parcial” y 0.0 si la respuesta se evaluó con “No”. Cada artículo obtuvo un puntaje de 0 a 3 puntos. Si un artículo tiene un puntaje igual o superior a 2, será seleccionado para extraer su información.

g. Resultados

En esta sección se resume los resultados obtenidos de la revisión sistemática en los siguientes pasos:

1. Se ejecutó las cadenas de búsqueda en cada base de datos seleccionada (IEEE, y Scopus), se obtuvieron 93 artículos.
2. De los 93 documentos, existieron 7 artículos duplicados (7.53%)
3. Los artículos fueron revisados y analizados en su título y resumen, tomando en consideración los criterios de inclusión y exclusión. De los 86 documentos revisados se seleccionaron 28 artículos, y 58 se descartaron al ser irrelevantes a las preguntas de investigación planteadas y a los criterios de inclusión.

   En la TABLA 1, se puede observar el proceso de selección en cada etapa

TABLA 1: *Resultados de la búsqueda en las bases de datos*

Base de Datos	***Artículos***					
	E1	***D***	***R***	***E2***	***S***	***%***
IEEEXplore	54	4	50	35	15	53,57
Scopus	39	3	36	23	13	46,43
Total	93	7	86	58	28	100

Dónde: *"E1"* significa artículos encontrados, *"D"* artículos duplicados, *"R"* artículos revisados, *"E2"* artículos eliminados, *"S"* artículos seleccionados.

4. Se aplicó las preguntas de calidad, y todos los artículos tuvieron promedio superior a 1.5, siendo así seleccionados todos. (ver TABLA 2).

TABLA 2: *Evaluación de calidad de cada artículo*

Artículo	Preguntas			Puntaje
	QA1	QA2	QA3	
AR01	1	1	1	3
AR02	1	1	1	3
AR03	1	1	1	3
AR04	1	1	1	3
AR05	1	1	1	3
AR06	0.5	1	1	2.5
AR07	1	1	1	3
AR08	0.5	1	1	2.5
AR09	1	1	1	3
AR10	1	1	0.5	2.5
AR11	0.5	1	1	2.5
AR12	0.5	1	1	2.5
AR13	0.5	1	1	2.5
AR14	0.5	1	1	2.5
AR15	0.5	1	1	2.5
AR16	0.5	0.5	1	2
AR17	0.5	1	1	2.5
AR18	0.5	1	1	2.5
AR19	0.5	1	1	2.5
AR20	1	1	1	3
AR21	0	1	1	2
AR22	1	1	1	3
AR23	0	1	1	2
AR24	0.5	1	1	2.5
AR25	1	1	1	3
AR26	0.5	1	1	2.5
AR27	1	1	1	3
AR28	0	1	1	2

INFORME DE MAPEO SISTEMÁTICO

Se han selecciona 28 artículos para analizarlos y dar contestación a las preguntas de investigación:

La FIGURA 1 representa la respuesta a la MQ1 "**¿Cuántos estudios se publicaron a lo ¿Cuántos estudios se publicaron a lo largo de los años en el área de ingeniería social?**" Se puede observar por año cuántos artículos se han publicado. Cabe destacar que no existen artículos escogidos que hayan sido publicados en el año 2019.

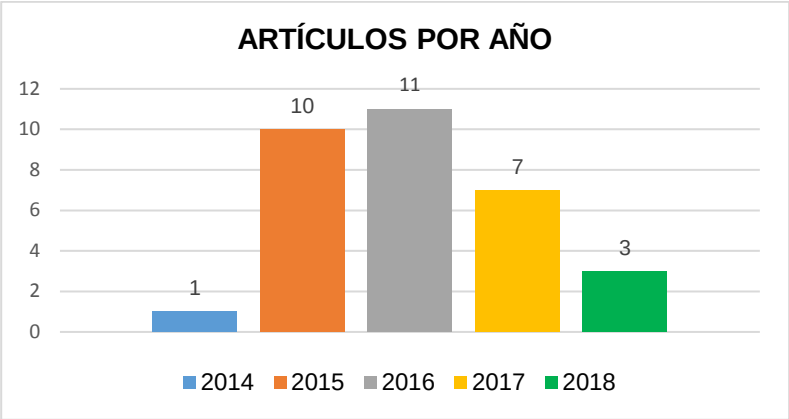


FIGURA 1: *MQ1*

Para responder a la MQ2 "**¿Cuáles son los autores más relevantes y activos en esta área?**", se identificaron los autores a partir de los trabajos seleccionados. No existen investigadores que hayan aparecido más de una vez en los resultados, el nombre de los autores y las publicaciones relacionadas son ilustradas en la TABLA 3.

TABLA 3: *NOMBRE DE LOS AUTORES Y LAS PUBLICACIONES RELACIONADAS*

Nombre	***Total***
Surbhi Gupta; Abhishek Singhal; Akanksha Kapoor; Andrea Cullen; Lorna Armitage; Zrinka Lovrić Švehla; Ivan Sedinić; Luka Pauk; Taimur Bakhshi; Ibrahim Ghafir; Vaclav Prenosil; Ahmad Alhejailan; Mohammad Hammoudeh; C. E. López Grande; R. S. Guadrón; Aisha Suliaman Alazri; Kavinga Yapa Abeywardana ; Eckhard Pfluegel ; Martin J. Tunnicliffe; Heidi Wilcox; Maumita Bhattacharya; Richard McEvoy; Stewart Kowalski; Mario Silic; Andrea Back; Van Vuuren I. E.; Kritzinger E.; Mueller C.; Wilcox H.; Bhattacharya M.; Curtis C. Campbell; Julián Andrés Vizcaíno Rodríguez; Dongmin Choi; Xin Su; Chang Cho; Pablo L. Gallegos-Segovia; Jack F. Bravo-Torres; Víctor M. Larios-Rosillo; Paul E. Vintimilla-Tapia; Ivan F. Yuquilima-Albarado; Juan D. Jara-Saltos; Azah Anir Norman; Maw Maw Hanifa; Suraya Ika Tamrin ; Suraya Hamid; Bharat Arya; K. Chandrasekaran; Ram Bhakta; Ian G. Harris; Jema David Ndibwile; Youki Kadobayashi; Doudou Fall; S.A.D.T.P. Kaushalya; R. M. R. S. B. Randeniya; A. D. S. Liyanage; B. B. Gupta1 Nalin; A. G. Arachchilage; Kostas E. Psannis; Senturk S; Yerli E; Sogukpinar I; AHMED ALEROUD; JORDAN LINA ZHOU; Anjum N. Shaikh; Antesar M. Shabut ; M.A. Hossain; Al-Sharif S; Iqbal F; Baker T; Khattack A.; Tushar Bhardwaj; Tarun Kumar Sharma; Manu Ram Pandit.	1

En cuanto a la MQ3 "**¿Cuáles son las revistas y congresos que se han publicado en el área mencionada?**", la FIGURA 2 muestra en qué lugar se publicaron los trabajos

seleccionados. Se publicaron 16 artículos en conferencias (66,67%) y 8 en revistas (33,33%).

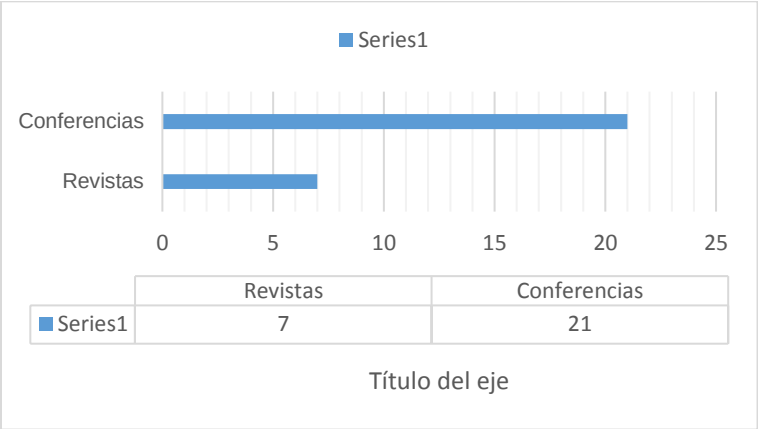


FIGURA 2: *Lugar se publicaron de los artículos seleccionados*

En la TABLA 4 muestra los 28 artículos seleccionados donde se detalla los nombres de los autores, el título, el año de publicación y su fuente de publicación (nombre del congreso o revista) dando contestación a las preguntas del mapeo sistemático MQ1, MQ2, MQ3.

TABLA 4: *Artículos Seleccionados*

CÓDIGO	AUTORES	TÍTULO	AÑO	REVISTA/CONGRESO
AR01	Surbhi Gupta; Abhishek Singhal; Akanksha Kapoor	A Literature Survey on Social Engineering Attacks: Phishing Attack.	2016	Conferencia Internacional de Informática, Comunicación y Automatización
AR02	Andrea Cullen; Lorna Armitage	The Social Engineering Attack Spiral (SEAS)	2016	Conferencia Internacional sobre Ciberseguridad y Protección de Servicios Digitales (Ciberseguridad).
AR03	Zrinka Lovrić Švehla; Ivan Sedinić; Luka Pauk	Going White Hat: Security Check by Hacking Employees Using Social Engineering Techniques.	2016	Convención Internacional sobre Tecnología de la Información y la Comunicación, Electrónica y Microelectrónica (MIPRO)
AR04	Taimur Bakhshi	Social Engineering: Revisiting End-User Awareness and Susceptibility to Classic Attack Vectors.	2017	Conferencia Internacional sobre Tecnologías Emergentes (ICET).
AR05	Ibrahim Ghafir; Vaclav Prenosil; Ahmad Alhejailan; Mohammad Hammoudeh	Social Engineering Attack Strategies and Defence Approaches.	2016	Conferencia internacional sobre la Internet del futuro de las cosas y la nube
AR06	C. E. López Grande; R. S. Guadrón	Social Engineering: The Silent Attack. [6]	2015	TRIGÉSIMA QUINTA CONVENCIÓN CENTRO AMERICANA Y PANAMEÑA DEL IEEE 2015 (CONCAPAN XXXV)

AR07	Aisha Suliaman Alazri	The Awareness of Social Engineering in Information Revolution: Techniques and Challenges.	2015	Conferencia Internacional sobre la Tecnología de Internet y las Transacciones Garantizadas (ICITST-2015)
AR08	Kavinga Yapa Abeywardana; Eckhard Pfluegel ; Martin J. Tunnicliffe	A Layered Defense Mechanism for a Social Engineering Aware Perimeter	2016	Conferencia de Informática de la EFS 2016
AR09	Heidi Wilcox; Maumita Bhattacharya	A Framework to Mitigate Social Engineering through Social Media within the Enterprise.	2016	Conferencia sobre Electrónica Industrial y Aplicaciones (ICIEA)
AR10	Richard McEvoy; Stewart Kowalski	Beyond Training and Awareness: From Security Culture to Security Risk Management.	2017	Negocios, Informática
AR11	Mario Silic; Andrea Back	The dark side of social networking sites: Understanding phishing risks.	2016	ELSEVIER
AR12	Van Vuuren I. E.; Kritzinger E.; Mueller C.	Identifying Gaps in IT Retail Information Security Policy Implementation Processes.	2016	Conferencia sobre seguridad de la información y ciberforense (InfoSec).
AR13	Wilcox H.; Bhattacharya M.	Countering Social Engineering through Social Media: An Enterprise Security Perspective.	2015	Lecture Notes in Computer Science
AR14	Curtis C. Campbell	Solutions for counteracting human deception in social engineering attacks.	2018	Emerald Insight
AR15	Julián Andrés Vizcaíno Rodríguez	Social engineering. Practice of confidential information obtained.	2015	Revista Síntesis Semilleros de Investigación

AR16	Dongmin Choi; Xin Su; Chang Cho	Invisible Secure Keypad Solution Resilient against Shoulder Surfing Attacks.	2016	Conferencia internacional sobre servicios móviles y de Internet innovadores en computación ubicua
AR17	Pablo L. Gallegos-Segovia; Jack F. Bravo-Torres; Víctor M. Larios-Rosillo; Paul E. Vintimilla-Tapia; Ivan F. Yuquilima-Albarado; Juan D. Jara-Saltos	Social engineering as an attack vector for ransomware.	2017	Conferencia CHILEANA de Ingeniería Eléctrica, Electrónica, Tecnologías de la Información y las Comunicaciones (CHILECON).
AR18	Azah Anir Norman; Maw Maw Hanifa; Suraya Ika Tamrin ; Suraya Hamid	Security Threats and Techniques in Social Networking Sites: A Systematic Literature Review	2017	Conferencia de Tecnologías del Futuro (FTC)
AR19	Bharat Arya; K. Chandrasekaran	A client-side anti-pharming (CSAP) approach.	2016	Conferencia Internacional sobre Tecnologías de Circuitos, Potencia e Informática (ICCPCT).
AR20	Ram Bhakta; Ian G. Harris	Semantic analysis of dialogs to detect social engineering attacks.	2015	Conferencia Internacional sobre Computación Semántica (IEEE ICSC 20 IS)
AR21	Jema David Ndibwile; Youki Kadobayashi; Doudou Fall	UnPhishMe: Phishing Attack Detection by Deceptive Login Simulation through an Android Mobile App.	2017	Conferencia Conjunta de Asia sobre Seguridad de la Información (AsiaJCIS).
AR22	S.A.D.T.P. Kaushalya; R. M. R. S. B. Randeniya; A. D. S. Liyanage	An Overview of Social Engineering in the Context of Information Security.	2018	Conferencia Internacional sobre Tecnologías de la Ingeniería y Ciencias Aplicadas

AR23	B. B. Gupta1 Nalin; A. G. Arachchilage; Kostas E. Psannis	Defending against phishing attacks: taxonomy of methods, current issues and future directions.	2018	Springer Science+Business Media
AR24	Senturk S; Yerli E; Sogukpinar I	Email phishing detection and prevention by using data mining techniques.	2017	Conferencia Internacional de Ingeniería Informática (UBMK)
AR25	AHMED ALEROUD; JORDAN LINA ZHOU	Phishing Environments, Techniques, and Countermeasures: A Survey.	2017	Diario Informática y Seguridad
AR26	Anjum N. Shaikh; Antesar M. Shabut ; M.A. Hossain	A literature review on phishing crime, prevention review and investigation of gaps.	2017	Conferencia Internacional sobre Software, Conocimiento, Gestión de la Información y sus Aplicaciones (SKIMA)
AR27	Al-Sharif S; Iqbal F; Baker T; Khattack A.	White-hat hacking framework for promoting security awareness.	2016	Conferencia Internacional de la IFIP sobre Nuevas Tecnologías, Movilidad y Seguridad (NTMS).
AR28	Tushar Bhardwaj; Tarun Kumar Sharma; Manu Ram Pandit	Social Engineering Prevention by Detecting Malicious URLs Using Artificial Bee Colony Algorithm.	2014	Conferencia Internacional sobre Soft Computing for Problem Solving, Advances in Intelligent Systems and Computing

INFORME DE REVISIÓN SISTEMÁTICA

A. Extracción de la Información.

Los criterios de selección de estudios establecen la pauta de extracción de información relevante de los 28 artículos seleccionados. Por cada uno se sintetizó y clasificó a cada artículo para tener una visión clara de las preguntas RQ1 y RQ2 como se describe en la TABLA 5.

TABAL 5: *Categorías de selección de información*

Técnicas de ataque bajo la modalidad de Ingeniería Social	PHISHING	T01
	BAITING	T02
	SMISHING	T03
	QUID PRO QUO	T04
	PRETEXTING	T05
	PHARMING	T06
	VHISHING	T07
	SPEAR-PHISHING	T08
	DUMPSTER DIVING	T09
	SHOULDER SURFING	T10
	ESPIONAJE INDUSTRIAL	T11
	TAILGATING	T12
	SCAREWARE	T13
Métodos o técnicas para mitigar ciberataques bajo la modalidad de ingeniería social	Estándares	S01
	Educación, Capacitación, y Concientización	S02
	Técnicas de seguridad lógica	S03
	Herramientas antiphishing	S04
	Técnicas de autenticación	S05
	Estrategias de contratación y empleo	S06
	Políticas	S07
	Técnicas de seguridad física	S08
	Pruebas de penetración	S09
	Estatutos legales	S10
	Protocolos	S11

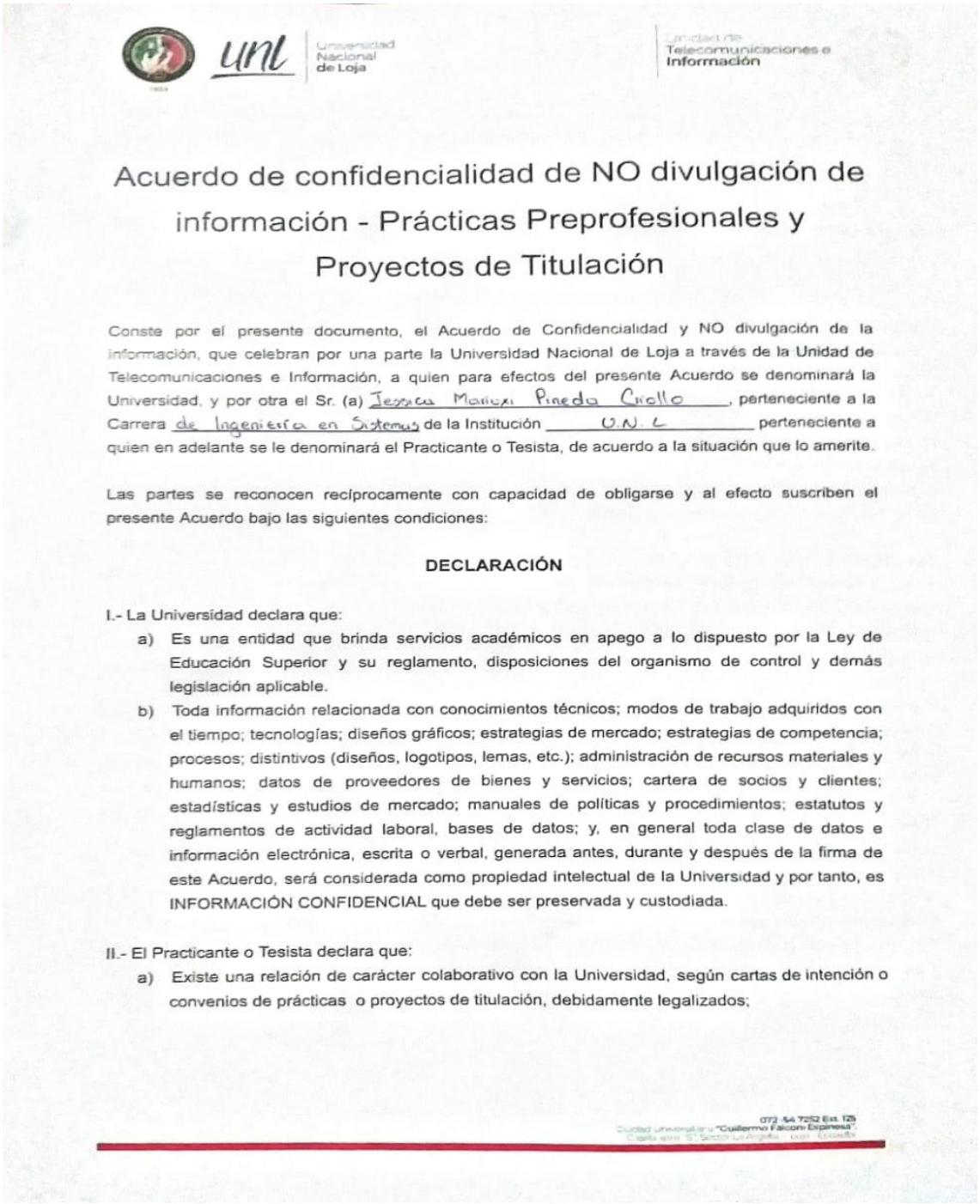
TABLA 6: *Matriz por artículo y clasificación por artículo*

ART	TÉCNICAS DE ATAQUE													SALVAGUARDIAS (Métodos para mitigar)										
	T 1	T 2	T 3	T 4	T 5	T 6	T 7	T 8	T 9	T 10	T 11	T 12	T 13	S01	S02	S03	S04	S05	S06	S07	S08	S09	S10	S11
AR01	x													x	x	x	x	x						
AR02	x						x					x		x	x				x	x				x
AR03	x			x		x									x					x				
AR04	x							x							x									
AR05	x				x	x						x	x							x	x			x
AR06	x	x	x	x	x	x									x					x		x		
AR07	x			x				x	x	x					x					x			x	
AR08	x	x		x			x				x												x	
AR09	x													x	x					x				
AR10															x									
AR11	x														x							x		x
AR12	x													x	x					x				x
AR13	x					x								x	x	x				x		x		
AR14															x					x				x
AR15		x													x									
AR16										x														
AR17	x					x									x	x								
AR18	x														x	x				x			x	
AR19	x					x										x		x						
AR20	x																x	x						
AR21	x															x	x	x						
AR22	x	x		x	x							x			x					x	x			

TABLA 6: *Matriz por artículo y clasificación por artículo*

ART	TÉCNICAS DE ATAQUE													SALVAGUARDIAS (Métodos para mitigar)									
	T 1	T 2	T 3	T 4	T 5	T 6	T 7	T 8	T 9	T 10	T 11	T 12	T 13	S01	S02	S03	S04	S05	S06	S07	S08	S09	S10	S11
AR01	x													x	x	x	x	x						
AR23	x														x	x		x						
AR24	x	x			x		x	x				x				x	x							
AR25	x						x									x		x						
AR26	x														x	x	x		x					
AR27	x					x																x		
AR28	x					x												x						

Anexo 3: Acuerdo de confidencialidad



Universidad Nacional de Loja

Unidad de Telecomunicaciones e Información

Acuerdo de confidencialidad de NO divulgación de información - Prácticas Preprofesionales y Proyectos de Titulación

Conste por el presente documento, el Acuerdo de Confidencialidad y NO divulgación de la información, que celebran por una parte la Universidad Nacional de Loja a través de la Unidad de Telecomunicaciones e Información, a quien para efectos del presente Acuerdo se denominará la Universidad, y por otra el Sr. (a) Jessica Marlexi Pineda Criollo, perteneciente a la Carrera de Ingeniería en Sistemas de la Institución U.N.L perteneciente a quien en adelante se le denominará el Practicante o Tesista, de acuerdo a la situación que lo amerite.

Las partes se reconocen recíprocamente con capacidad de obligarse y al efecto suscriben el presente Acuerdo bajo las siguientes condiciones:

DECLARACIÓN

I.- La Universidad declara que:

a) Es una entidad que brinda servicios académicos en apego a lo dispuesto por la Ley de Educación Superior y su reglamento, disposiciones del organismo de control y demás legislación aplicable.

b) Toda información relacionada con conocimientos técnicos; modos de trabajo adquiridos con el tiempo; tecnologías; diseños gráficos; estrategias de mercado; estrategias de competencia; procesos; distintivos (diseños, logotipos, lemas, etc.); administración de recursos materiales y humanos; datos de proveedores de bienes y servicios; cartera de socios y clientes; estadísticas y estudios de mercado; manuales de políticas y procedimientos; estatutos y reglamentos de actividad laboral, bases de datos; y, en general toda clase de datos e información electrónica, escrita o verbal, generada antes, durante y después de la firma de este Acuerdo, será considerada como propiedad intelectual de la Universidad y por tanto, es INFORMACIÓN CONFIDENCIAL que debe ser preservada y custodiada.

II.- El Practicante o Tesista declara que:

a) Existe una relación de carácter colaborativo con la Universidad, según cartas de intención o convenios de prácticas o proyectos de titulación, debidamente legalizados;

072-54 7252 Ext. 125

b) Para desempeñar las funciones dentro de sus prácticas o para la ejecución del proyecto de titulación, tendrá acceso a información privilegiada, la cual acepta guardar con escrupulosa confidencialidad.

En virtud de lo anterior, ambas partes se someten a las disposiciones siguientes:

CLÁUSULAS

PRIMERA. Ambas partes aceptan que la información señalada en la declaración I-b), es propiedad de la Universidad y de UTI, la misma será considerada como INFORMACIÓN CONFIDENCIAL, por lo tanto, el Practicante o Tesista se obliga a custodiarla, conservarla y a no divulgarla a terceros, ya sea en forma verbal, escrita, por medios electrónicos, magnéticos, o por cualquier otro medio, directa o indirectamente.

La obligación asumida por el Pasante o Tesista mediante el presente acuerdo, permanecerá durante la vigencia del período de sus Pasantías o hasta la culminación de su proyecto de titulación, extendiéndose por tiempo indefinido luego de finalizada su vinculación colaborativa, indistintamente de las funciones que haya ocupado, dentro de la UTI.

SEGUNDA. La Universidad entregará al Practicante o Tesista los implementos de trabajo necesarios para cumplir con sus objetivos, así como las credenciales de acceso a los diferentes sistemas y/o aplicativos que requiera de acuerdo a la naturaleza de sus actividades. El nombre de usuario que se le asigne quedará registrado en todas las operaciones que realice en los sistemas y/o aplicativos a los que ingrese.

El usuario y contraseña serán remitidos al Practicante o Tesista vía correo electrónico. El cambio de contraseña, la administración y mantenimiento de las credenciales de acceso se realizará de acuerdo a las políticas y procedimientos que en materia de seguridad de la información establezca la Universidad.

TERCERA. El objetivo principal del presente Acuerdo es proteger toda información de índole financiera, comercial, técnica, laboral, académica que tenga carácter confidencial, y que se relacione con productos, servicios, procesos, proyectos, sistemas de información, nuevas tecnologías, talento humano, planificación estratégica y operativa, clientes de la Universidad.

Por tanto, las partes se comprometen a aplicar las medidas de seguridad estipuladas en la normativa interna para evitar la divulgación, reproducción, fuga o uso no autorizado de información confidencial o patentada; y, a custodiar la información en lugares de acceso limitado únicamente a personas autorizadas.

CUARTA. El Practicante o Tesista reconoce y acepta que el incumplimiento de las obligaciones contraídas en el presente Acuerdo implicará asumir las sanciones establecidas en Reglamento

Interno de la Universidad, sin perjuicio de las acciones civiles o penales que la Universidad pudiera tomar en su contra.

QUINTA. Este Acuerdo deberá ser legalizado y archivado por el Director de la UTI. Una copia del Acuerdo se entregará al Practicante o Tesista y otra al Responsable de Seguridad de la Información.

SEXTA.- El presente Acuerdo no aplicará en los siguientes casos:

a) Por el consentimiento previo y escrito de la Universidad o de la UTI;
b) Cuando la información confidencial haya pasado a dominio público por razones distintas al incumplimiento de las obligaciones constantes en el presente Acuerdo;
c) Cuando exista requerimiento de autoridad competente que obligue al Practicante o Tesista a entregar la información que se encuentra a su cargo, y previo conocimiento y autorización del Director de la UTI.

SÉPTIMA. Si alguna de las estipulaciones del presente documento llegare a ser ilegal, inválida o sin vigencia, debido a modificaciones a la legislación ecuatoriana, dicha cláusula deberá excluirse, y este Acuerdo, en el alcance de lo posible y sin destruir su propósito, será ejecutado como si dicha estipulación, no hubiera hecho parte del mismo. Las restantes disposiciones aquí contenidas deberán conservar el mismo valor y efecto, sin afectación directa o indirecta, por la disposición ilegal, inválida o sin vigencia.

LAS PARTES han determinado la importancia de mantener la integridad, disponibilidad y confidencialidad de la información propiedad de la Universidad Nacional de Loja; han leído y comprendido las estipulaciones de este Acuerdo; y, se comprometen a cumplir los términos y condiciones del mismo, para lo cual lo suscriben en Loja, a los 8 del mes de Febrero del año 2019.

No. CI: 1104959547
PRACTICANTE ( ) TESISTA (X)

Ing. Jhon A. Calderón Sanmartín
DIRECTOR U.T.I.

UNL

Anexo 4: Análisis de Riesgos.

ANALISIS DE RIESGOS

Se realizó el análisis de riesgo basado en la Metodología Margerit v3 (ver FIGURA 3 del TT). Así mismo en base al catálogo de elementos de la Metodología Margerit v3 se han establecido los niveles BAJO, MODERADO, ALTO, y CRÍTICO para la "Probabilidad de Ocurrencia", el "Impacto", y la "Valoración del Riesgo". A continuación, se presenta los resultados del proceso realizado:

1) IDENTIFICACIÓN DEL ACTIVO

El activo identificado para el proceso de análisis de riesgos fue el usuario, el cual está representado por los estudiantes, docentes, administrativos y empleados de la comunidad universitaria. Esto debido a que el éxito de un ciberataque bajo la modalidad de Ingeniería Social consiste en explotar las vulnerabilidades humanas para sustraer información.

2) IDENTIFICACIÓN DE AMENAZAS

Se identificó a las técnicas mostradas en la TABLA 5 del TT como las principales amenazas bajo la modalidad de ingeniería social a las cuales podrían estar expuesto el usuario.

3) CRITERIOS DE VALORACIÓN

- **Probabilidad de ocurrencia (P.O.)**

Se define la probabilidad de ocurrencia para cada amenaza tomando en cuenta los siguientes criterios de valoración:

TABLA 1: *Valoración de la probabilidad de ocurrencia*

Criterios a considerar para determinar la probabilidad de ocurrencia		
Probabilidad	**Descripción**	**Valor**
BAJO	La materialización de la amenaza ocurre solo bajo circunstancias excepcionales.	1
MODERADO	Es poco probable que la amenaza sea materializada, es decir, que se podría presentar alguna vez.	2
ALTO	Es probable que la amenaza sea materializada, es decir, que se podría presentar varias veces.	3
CRÍTICO	Es muy probable que la amenaza sea materializada, es decir que se podría presentar con mucha frecuencia.	4

- **Impacto (I)**

Se define el impacto que puede tener la materialización de las amenazas de Ingeniería Social, con la descripción de los siguientes niveles:

TABLA 2: *Valoración del Impacto*

Criterios a considerar para determinar el impacto		
Impacto	**Descripción**	**Valor**
BAJO	Cuando la amenaza se materializa y no afecta a los principios (confidencialidad, integridad, y disponibilidad) de la información.	[1 - 3]
MODERADO	Cuando la amenaza se materializa afectando a uno de los principios (confidencialidad, integridad, y disponibilidad) de la información.	[4 - 6]
ALTO	Cuando la amenaza se materializa afectando a dos principios (confidencialidad, integridad, y disponibilidad) de la información.	[7 - 9]
CRÍTICO	Cuando la amenaza se materializa afectando a la información en sus tres principios (confidencialidad, integridad, y disponibilidad).	[10 - 12]

La valoración del impacto se realiza en base a los principios de la Seguridad de la Información:

- **Confidencialidad:** Mide el impacto que tendría la pérdida de confidencialidad de la información, es decir, que la información sea conocida por personas no autorizadas.

TABLA 3: *Valoración del Impacto sobre la confidencialidad*

Criterios a considerar para determinar el impacto sobre la CONFIDENCIALIDAD		
Impacto	**Descripción**	**Valor**
BAJO	Cuando la información obtenida por el atacante es accesible a todo el público.	1
MODERADO	Cuando la información obtenida por el atacante es de uso interno, es decir, que está disponible para todos los empleados y terceros seleccionados.	2
ALTO	Cuando la información obtenida por el atacante es confidencial, es decir, que la información es sensible y solamente puede ser conocida al interior de la institución.	3
CRÍTICO	Cuando la información obtenida por el atacante es restringida, es decir, que solo puede ser accedida por grupos específicos de usuarios que requieren del conocimiento de esta información para estricto cumplimiento de sus funciones.	4

- **Integridad:** Mide el impacto que tendría la pérdida de integridad, es decir, si la exactitud y estado completo de la información o sus métodos de procesamiento fueran alterados.

TABLA 4: *Valoración del Impacto sobre la integridad*

Criterios a considerar para determinar el impacto sobre la INTEGRIDAD		
Impacto	**Descripción**	**Valor**
BAJO	No afecta a la Integridad de la información.	1
MODERADO	Cuando el atacante afecta información no relevante y netamente informativa.	2
ALTO	Cuando el atacante afecta información que proporciona datos personales, instrucciones, directrices, etc. para el desempeño de las actividades que realiza la institución.	3
CRÍTICO	Cuando el atacante afecta información crítica que no puede ser modificada o alterada sin la debida autorización y que pone en riesgo la continuidad del negocio.	4

- **Disponibilidad:** Mide el impacto que tendría la pérdida de disponibilidad, es decir, si los usuarios autorizados no tuvieran acceso a la información en el momento que lo requieran.

TABLA 5: *Valoración del Impacto sobre la disponibilidad*

Criterios a considerar para determinar el impacto sobre la DISPONIBILIDAD		
Impacto	**Descripción**	**Valor**
BAJO	No afecta a la Integridad de la información.	1
MODERADO	Cuando el atacante afecta información no relevante y netamente informativa.	2
ALTO	Cuando el atacante afecta información que proporciona datos personales, instrucciones, directrices, etc. para el desempeño de las actividades que realiza la institución.	3
CRÍTICO	Cuando el atacante afecta información crítica que no puede ser modificada o alterada sin la debida autorización y que pone en riesgo la continuidad del negocio.	4

4) VALORACIÓN DEL RIESGO (V.R.)

Con base en la valoración de la probabilidad de ocurrencia y del impacto, se establecen los siguientes niveles de riesgo:

TABLA 6: *Valoración del Riesgo*

Criterios a tomar en cuenta para identificar el riesgo		
Riesgo	**Descripción**	**Valor**
BAJO	Si la amenaza materializada no afecta sobre la confidencialidad, integridad y disponibilidad de la información. Su tiempo de recuperación no necesariamente será inmediato.	[1 - 12]
MODERADO	Si la amenaza materializada afecta de forma temporal la confidencialidad, integridad o disponibilidad de la información. Su tiempo de recuperación será un periodo corto.	[13 - 24]
ALTO	Si la amenaza materializada afecta parcialmente sobre la confidencialidad, integridad o disponibilidad de la información. Su tiempo de recuperación es considerable.	[25 - 36]
CRÍTICO	Si la amenaza materializada afecta gravemente sobre la confidencialidad, integridad o disponibilidad de la información. Su tiempo de recuperación es extenso y en el peor de los casos no se podría retomar con normalidad las actividades de la institución.	[37 - 48]

Una vez establecidos los niveles de riesgo, se identifica las zonas de riesgo aceptable e inaceptable para la institución en el siguiente Mapa de Calor:

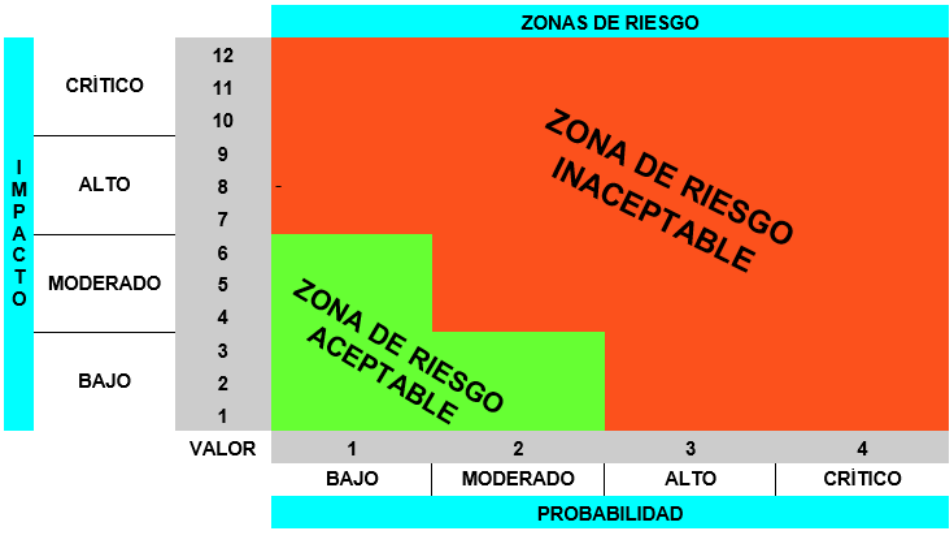


FIGURA 1: *Mapa de calor de las zonas de riesgo*

- **Zona de riesgo aceptable**: El riesgo se encuentra en un nivel bajo, es decir que el riesgo presentado podrá ser mitigado por los controles que posee la institución.
- **Zona de riesgo inaceptable**: El riesgo se encuentra en un nivel moderado, alto o crítico. Requiere acciones inmediatas, es decir, que el departamento de TI de la institución deberá mejorar o complementar los controles existentes en la institución.

La TABLA 4 presenta la valoración del riesgo para cada amenaza de ingeniería social identificada.

TABLA 7: *Valoración del Riesgo de las amenazas de Ingeniería Social identificadas.*

COD	AMENAZAS	P.O.	VALORACION DEL IMPACTO			I	V.R.
			CONF.	INTE.	DISP.		
A01	PHISHING	4	4	3	1	8	**32**
A02	BAITING	2	3	3	1	7	**14**
A03	SMISHING	3	4	1	1	6	**18**
A04	Quid Pro Quo	3	3	1	1	5	**15**
A05	PRETEXTING	2	3	1	1	5	**10**
A06	PHARMING	1	3	4	1	8	**8**
A07	VHISHING	3	3	1	1	5	**15**
A08	SPEAR-PHISHING	3	4	3	1	8	**24**
A09	DUMPSTER DIVING	1	4	1	1	6	**6**
A10	SHOULDER SURFING	3	2	1	1	4	**12**
A11	ESPIONAJE INDUSRIAL	2	3	1	1	5	**10**
A12	TAILGATING	4	4	3	3	10	**40**
A13	SCAREWARE	2	3	3	1	7	**14**

La valoración del riesgo para cada amenaza de Ingeniería Social se obtuvo de la siguiente manera:

Se establecio el valor para la **PROBABILIDAD DE OCURRENCIA** en base a la valoracion establecida en la TABLA 1**;** luego tomando en cuenta la valoracion de la TABLA 2 se asigno un valor para cada uno de los principios de la Seguridad de la Información: Confidencialidad, Integridad, y Disponibilidad, y posteriroemente se realizo la sumatoria de estos principios para obtener el valor del **IMPACTO**. Finalmente, para obtener el valor del riesgo se multiplica el valor de la **PROBABILIDAD DE OCURRENCIA** por el valor del **IMPACTO.**

En el siguiente mapa de calor se identifica la zona de riesgo en la que se encuentra cada amenaza de Ingenieria Social, esto en base a las zonas de riesgo aceptable e inaceptable identificadas para la institución.

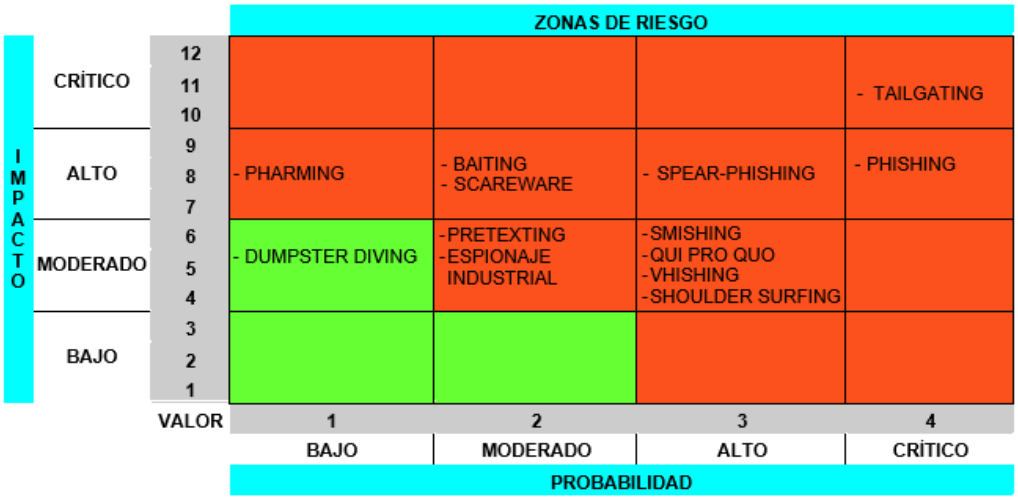


FIGURA 2: *Ubicación de las amenazas de Ingeniería Social en el mapa de calor.*

5) SALVAGUARDAS (S)

En base al estándar ISO/IEC 27002:2013 y tomando en cuenta las salvaguardas identificadas en la SRL, los controles y contramedidas para reducir o mitigar ciberataques bajo la modalidad de Ingeniería Social son las siguientes:

TABLA 8: *Controles para mitigar amenazas de Ingeniería Social.*

SALVAGUARDIAS ISO/IEC 27002:2013	
OBJETIVO DE CONTROL	**CONTROL**
5. POLÍTICAS DE SEGURIDAD	
5.1 Directrices de la Dirección en seguridad de la información	**5.1.1 Conjunto de políticas para la seguridad de la información:** Establecer políticas para la seguridad del usuario y de la información que maneja de acuerdo a las necesidades identificadas en el análisis de riesgos, las mismas que deben ser aprobadas por la dirección de TI para posteriormente ser difundidas a la toda la comunidad universitaria.
	5.1.2 Revisión de las políticas para la seguridad de la información: El departamento de TI de la institución debe definir un plan de revisiones para garantizar que las políticas cumplan con el propósito para el cual fueron creadas. El cual debe estar bajo la responsabilidad del experto en seguridad.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	
6.1 Organización interna	**6.1.1. Asignación de responsabilidades para la seguridad de la información:** Definir y asignar de manera clara los roles y responsabilidades de cada usuario perteneciente a la comunidad universitaria.
	6.1.2 Segregación de tareas: Realizar la separación de las funciones asignando distintos perfiles o áreas de responsabilidad para evitar usos o accesos indebidos a la información o a las aplicaciones o sistemas que la gestionan (activos de información) mediante la separación de las funciones asignando distintos perfiles o áreas de responsabilidad.
6.2 Dispositivos para movilidad y teletrabajo	**6.2.1 Política de uso de dispositivos para movilidad:** Para el uso de celulares, tablets, portátiles u otros dispositivos de uso personal se debe establecer una política formal y adoptar medidas de seguridad adecuadas para la protección contra los riesgos de Ingeniería Social.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	
7.1 Antes de la contratación	**7.1.1 Investigación de antecedentes:** Como parte de los métodos de reclutamiento, selección, y contratación de los nuevos docentes, administrativos, o empleados se debe realizar la verificación de antecedentes personales, académicos, laborales, penales, policiales, judiciales, y su buro de crédito.
	7.1.2 Términos y condiciones de contratación: Los acuerdos contractuales con los docentes, administrativos, empleados y terceros establecerá sus obligaciones y las obligaciones de la institución; evitando deslindarse de la responsabilidad ante un acontecimiento delictivo de Ingeniería Social.

7.2 Durante la contratación	**7.2.1 Responsabilidades de gestión:** Establecer mecanismos para asegurar que los estudiantes, docentes, administrativos, empleados y terceros actúen en concordancia con las políticas y los procedimientos establecidos la seguridad del usuario y de la información que maneja.
	7.2.2 Concienciación, educación y capacitación en seguridad de la información: Adoptar medidas como la divulgación de políticas y manuales; difusión de incidentes y ataques, explicando sus causas y orígenes; creación de talleres en materia de prevención y detección de los riesgos de ingeniería social.
	7.2.3 Proceso disciplinario: Establecer un proceso disciplinario formal para tomar medidas contra los administrativos, docentes, empleados y terceros que se han involucrado en una transgresión de ingeniería social.
7.3 Cese o cambio de puesto de trabajo.	**7.3.1 Cese o cambio de puesto de trabajo:** Establecer mecanismos devolución de activos y eliminación de los derechos de acceso físico y lógicos ante el abandono o cambio de puesto por parte de los docentes, administrativos, o empleados.
8. GESTIÓN DE ACTIVOS	
8.1 Responsabilidad sobre los activos	**8.1.1 Inventario de activos:** Se deben identificar los activos o recursos asociados al usuario.
	8.1.3 Uso aceptable de los activos: Se debe identificar, documentar e implementar reglas para el buen uso de los activos o recursos asociados al usuario.
8.2 Clasificación de la información	**8.2.1. Directrices de clasificación:** Establecer métodos para la clasificación de la información en función de la integridad, confidencialidad y disponibilidad de la misma.
	8.2.2 Etiquetado y manipulado de la información: Establecer procedimientos para el etiquetado de acuerdo al esquema de clasificación de información adoptado por la institución.

	8.2.3 Manipulación de activos: Establecer procedimientos para la manipulación de la información de acuerdo al esquema de clasificación adoptado por la institución.
8.3 Manejo de los soportes de almacenamiento	**8.3.1 Gestión de soportes extraíbles:** Se debe restringir la conexión de celulares, tablets, portátiles, USB u otros dispositivos removibles de uso personal a la red de la institución sin la debida autorización.
9. CONTROL DE ACCESOS.	
9.2 Gestión de acceso de usuario	**9.2.1 Gestión de altas/bajas en el registro de usuarios:** Implementar métodos de registro y cancelación de accesos de un usuario, desde el registro inicial hasta su baja cuando ya no sea necesario su acceso.
	9.2.2 Gestión de los derechos de acceso asignados a usuario: Establecer procedimientos de control de acceso físico y lógico para los usuarios, con el fin de asegurar que los activos de información se mantengan protegidos.
	9.2.5 Revisión de los derechos de acceso de los usuarios: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.
	9.2.6 Retirada o adaptación de los derechos de acceso: Los derechos de acceso para todos estudiantes, docentes, administrativos, empleados y usuarios externos a la información y a las instalaciones se deberían eliminar al término de su empleo, contrato o acuerdo, o se deberían ajustar en caso de realizarse cambios en el empleo.
9.3 Responsabilidades del usuario.	**9.3.1 Uso de información confidencial para la autenticación:** La autenticación de cada usuario (estudiante, docente, administrativo, empleado, o tercero) para el ingreso a las instalaciones, información, sistemas, etc. debe ser única y no puede ser compartida.
	9.4.1. Restricción del acceso a la información: El acceso a la información de la institución se debe restringir de acuerdo con la política de control de acceso establecida previamente.

9.4 Control de acceso a sistemas y aplicaciones.	**9.4.2. Procedimientos seguros de inicio de sesión:** Establecer buenas prácticas de seguridad para el uso y protección de claves o contraseñas, las cuales constituyen un medio de validación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos de manera segura.
	9.4.5 Control de acceso al código fuente de los programas: El departamento de TI de la institución debe establecer mecanismos de protección para el código fuente de sus aplicativos desarrollados.
11. SEGURIDAD FÍSICA Y AMBIENTAL.	
11.1 Áreas seguras	**11.1.1 Perímetro de seguridad física:** Definir perímetros de seguridad para la protección de las áreas que contienen información confidencial o critica.
	11.1.2 Controles físicos de entrada: Implementar sensores de identificación como: analizadores de retina, tarjetas inteligentes, video cámaras, vigilantes jurados, etc. para acceder a las diferentes dependencias de la institución.
	11.1.3 Seguridad de oficinas, despachos y recursos: Diseñar y aplicar un sistema de seguridad física a las oficinas, salas e instalaciones de la organización.
11.2 Seguridad de los equipos.	**11.2.1 Emplazamiento y protección de equipos:** Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas de ingeniería social.
	11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla: Adoptar una política para evitar el acceso no autorizado a la información en los puestos de trabajo, como también a las instalaciones y a los equipos compartidos.

12. SEGURIDAD EN LA OPERATIVA.	
12.2 Protección contra código malicioso.	**12.2.1 Controles contra el código malicioso:** Establecer controles de detección y prevención contra el malware o código malicioso.
13. SEGURIDAD EN LAS TELECOMUNICACIONES.	
13.1 Gestión de la seguridad en las redes.	**13.1.1 Controles de red:** Establecer mecanismos (Configuraciones Seguras de Dispositivos de Red: Firewalls, Routers y Switches) para administrar y controlar las redes para proteger la información en sistemas y aplicaciones.
	13.1.2 Mecanismos de seguridad asociados a servicios en red: Se debe identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.
13.2 Intercambio de información con partes externas.	**13.2.1 Políticas y procedimientos de intercambio de información:** Establecer políticas, procedimientos y controles para proteger la transferencia de información mediante el uso de todo tipo de dispositivos de comunicación.
	13.2.2 Acuerdos de intercambio: Crear acuerdos para tratar la transferencia segura de información entre la institución y las partes externas.
	13.2.3 Mensajería electrónica: Emplear la política para el buen uso del correo electrónico desarrollada por la Unidad de Telecomunicaciones e Información de la Universidad. Además, se debe desarrollar una guía de buenas prácticas para el reconocimiento de ataques de phishing.

18. CUMPLIMIENTO.	
18.1 Cumplimiento de los requisitos legales y contractuales.	**18.1.1 Identificación de la legislación aplicable:** La legislación aplicable para tomar acciones entorno a la Ingeniería Social en la institución son: ✓ El Esquema Gubernamental de Seguridad de la Información EGSI. ✓ Las Políticas de Telecomunicaciones, Desarrollo de Software, Redes de La Universidad Nacional de Loja. ✓ La Ley de Comercio Electrónico, Firmas y Mensajes de Datos. ✓ Código Orgánico Integral Penal COIP. Los mismos que deben estar documentados y actualizados.
	18.1.2 Derechos de propiedad intelectual (DPI): Supervisar que el uso del software, la información propia de la institución o adquirida de terceros, y los aplicativos desarrollados estén de acuerdo a la Ley de Propiedad Intelectual del Ecuador.
	18.1.3 Protección de los registros de la organización: Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos.
	18.1.4 Protección de datos y privacidad de la información personal: Establecer una política para la protección de datos y privacidad de la información personal en base al modelo europeo de la Ley Orgánica de Protección de Datos Personales.

Teniendo en cuenta lo anterior descrito, la siguiente tabla muestra los controles y contramedidas que mitigan a cada amenaza de Ingeniería Social identificada:

TABLA 9: *Controles para mitigar cada amenaza de Ingeniería Social identificada.*

SALVAGUARDIAS ISO/IEC 27002:2013														
OBJETIVO DE CONTROL	**CONTROL**	**AMENAZAS QUE MITIGA EL CONTROL**												
		A 01	**A 02**	**A 03**	**A 04**	**A 05**	**A 06**	**A 07**	**A 08**	**A 09**	**A 10**	**A 11**	**A 12**	**A 13**
5. POLÍTICAS DE SEGURIDAD														
5.1 Directrices de la Dirección en seguridad de la información	5.1.1 Conjunto de políticas para la seguridad de la información	x	x	x	x	x	x	x	x	x	x	x	x	x
	5.1.2 Revisión de las políticas para la seguridad de la información	x	x	x	x	x	x	x	x	x	x	x	x	x
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN														
6.1 Organización interna	6.1.1. Asignación de responsabilidades para la seguridad de la información.	x	x	x	x	x	x	x	x	x	x	x	x	x
	6.1.2 Segregación de tareas	x	x	x	x	x	x	x	x	x	x	x	x	x
6.2 Dispositivos para movilidad y teletrabajo	6.2.1 Política de uso de dispositivos para movilidad		x	x				x						

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.														
7.1 Antes de la contratación	7.1.1. Investigación de antecedentes.					x					x	x		
	7.1.2 Términos y condiciones de contratación.											x		
7.2 Durante la contratación	7.2.1 Responsabilidades de gestión.	x	x	x	x	x	x	x	x	x	x	x	x	x
	7.2.2. Concienciación, educación y capacitación en seguridad de la información.	x	x	x	x	x	x	x	x	x	x	x	x	x
7.3 Cese o cambio de puesto de trabajo	7.2.3 Proceso disciplinario.	x	x	x	x	x	x	x	x	x	x	x	x	x
	7.3.1 Cese o cambio de puesto de trabajo.											x		
8. GESTIÓN DE ACTIVOS														
8.1 Responsabilidad sobre los activos	8.1.1 Inventario de activos.	x	x	x	x	x	x	x	x	x	x	x	x	x
	8.1.3 Uso aceptable de los activos.	x	x	x	x	x	x	x	x	x	x	x	x	x
8.2 Clasificación de la información	8.2.1 Directrices de clasificación.	x	x	x	x	x	x	x	x	x	x	x	x	x
	8.2.2 Etiquetado y manipulado de la información.	x	x	x	x	x	x	x	x	x	x	x	x	x
	8.2.3 Manipulación de activos.	x	x	x	x	x	x	x	x	x	x	x	x	x
8.3 Manejo de los soportes de almacenamiento.	8.3.1 Gestión de soportes extraíbles.		x											

9. CONTROL DE ACCESOS.														
9.2 Gestión de acceso de usuario	9.2.1 Gestión de altas/bajas en el registro de usuarios.											x		
	9.2.2 Gestión de los derechos de acceso asignados a usuarios.		x			x				x		x	x	
	9.2.5 Revisión de los derechos de acceso de los usuarios.											x		
	9.2.6 Retirada o adaptación de los derechos de acceso.											x		
9.3 Responsabilidades del usuario.	9.3.1 Uso de información confidencial para la autenticación.	x		x				x	x	x	x	x		
9.4 Control de acceso a sistemas y aplicaciones.	9.4.1. Restricción del acceso a la información	x		x	x	x		x	x	x	x	x	x	
	9.4.2. Procedimientos seguros de inicio de sesión	x		x					x		x	x	x	
	9.4.5 Control de acceso al código fuente de los programas.							x						

11. SEGURIDAD FÍSICA Y AMBIENTAL.														
11.1 Áreas seguras	11.1.1 Perímetro de seguridad física.		x							x	x	x	x	
	11.1.2 Controles físicos de entrada.		x							x	x	x	x	
	11.1.3 Seguridad de oficinas, despachos y recursos.		x							x	x	x	x	
11.2 Seguridad de los equipos.	11.2.1 Emplazamiento y protección de equipos.		x											
	11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.		x						x	x	x	x	x	
12. SEGURIDAD EN LA OPERATIVA.														
12.2 Protección contra código malicioso.	12.2.1 Controles contra el código malicioso.	x	x				x		x					x

13. SEGURIDAD EN LAS TELECOMUNICACIONES.														
13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red.						x							
	13.1.2 Mecanismos de seguridad asociados a servicios en red.	x					x		x					
13.2 Intercambio de información con partes externas.	13.2.1 Políticas y procedimientos de intercambio de información.	x		x	x	x		x	x			x		
	13.2.2 Acuerdos de intercambio.	x		x	x	x		x	x			x		
	13.2.3 Mensajería electrónica	x							x					
18. CUMPLIMIENTO														
18.1 Cumplimiento de los requisitos legales y contractuales.	18.1.1 Identificación de la legislación aplicable.	x	x	x	x	x	x	x	x	x	x	x	x	x
	18.1.2 Derechos de propiedad intelectual (DPI).											x		x
	18.1.3 Protección de los registros de la organización.					x				x		x	x	
	18.1.4 Protección de datos y privacidad de la información personal.	x	x	x	x	x	x	x	x	x	x	x	x	x

Anexo 5: Encuesta

a) Formato de la encuesta

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES
CARRERA DE INGENIERÍA EN SISTEMAS

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e Información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

Rol que desempeña: _____

Edad: ☐ 18 a 24 años
☐ 25 a 45 años
☐ 46 años en adelante

Sexo: ☐ Masculino
☐ Femenino

1. **¿Cuál es el uso que usted le da al Internet?**
   - ☐ Para trabajo
   - ☐ Para descargar archivos
   - ☐ Para ingresar a redes sociales
   - ☐ Para escuchar música.
   - ☐ Para realizar compras en línea.
   - ☐ Otros: _____

2. **Señale el/los navegadores de internet que usted utiliza.**

   - ☐ Chrome
   - ☐ Firefox
   - ☐ Safari
   - ☐ Internet Explorer
   - ☐ Opera
   - ☐ Otros: _____

3. ¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?

- ☐ Celulares
- ☐ Tablet
- ☐ Portátiles
- ☐ Computadoras de escritorio
- ☐ Otros: _____

4. ¿Usted hace uso de las redes sociales en su lugar de trabajo?

- ☐ Si
- ☐ No

Si su respuesta es "SI" señale que tipo de redes sociales utiliza:

- ☐ Facebook
- ☐ Whatsapp
- ☐ Telegram
- ☐ Twiteer
- ☐ Instagram
- ☐ Skype
- ☐ Mensajería Instantánea
- ☐ Correo Electrónico
- ☐ Otros: _____

5. ¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).

Mayúsculas	**A ..... Z**
Minúsculas	**a ..... z**
Símbolos	**/ # $ % & = ¿ ¡ ¿ ¡ | . - _ **
Números	**0 ..... 9**

- ☐ Mayúsculas y minúsculas
- ☐ Mayúsculas, minúsculas, y símbolos
- ☐ Mayúsculas, minúsculas, símbolos, y números.
- ☐ Mayúsculas y símbolos.
- ☐ Mayúsculas y números
- ☐ Minúsculas y símbolos.
- ☐ Minúsculas y números
- ☐ símbolos y números
- ☐ Solo mayúsculas
- ☐ Solo minúsculas
- ☐ Solo números
- ☐ Solo símbolos.

6. ¿Para que utiliza usted el correo electrónico asignado por la universidad?

- ☐ Para trabajo
- ☐ Para descargar archivos personales.
- ☐ Para el entretenimiento (descargar música, ver películas, jugar, etc)
- ☐ Para realizar compras en línea.
- ☐ Otro: _____

7. ¿Comparte usted información confidencial mediante el uso de las redes sociales?

☐ Si
☐ No

Si su respuesta es "SI" señale que tipo de información a compartido:

☐ Claves de tarjetas de crédito.
☐ Claves de cuentas electrónicas.
☐ Números de cuentas bancarias
☐ Números de tarjetas de crédito
☐ Número de cedula
☐ Documentos laborales
☐ Otro: _____

8. ¿Conoce usted acerca de la Ingeniería Social?

☐ Si
☐ No

Si su respuesta es "SI" haga una breve descripción :

_____
_____

9. ¿Conoce usted que es un delito informático?

☐ Si
☐ No

Si su respuesta es "SI" haga una breve descripción :

_____
_____

10. ¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?

☐ Si
☐ No

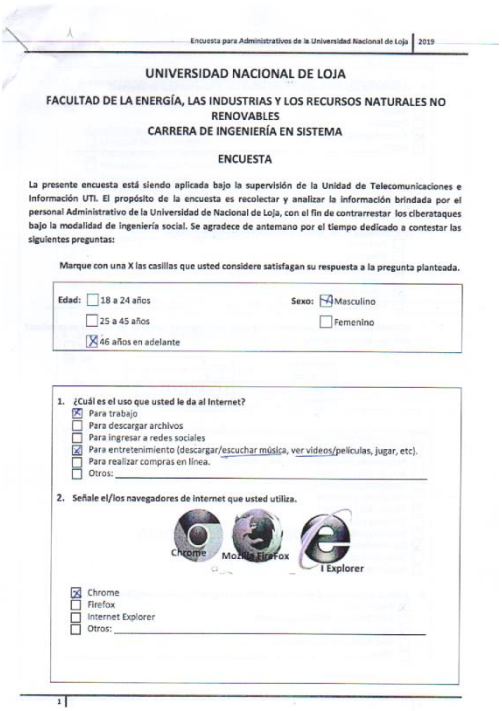
Si su respuesta es "SI" mencione la ley :_____

GRACIAS POR SU COLABORACIÓN

b) Encuestas aplicadas

Se adjunta como evidencia 30 de las 153 encuestas aplicadas.

- **Encuesta 001**



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMA

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e Información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

Edad: ☐ 18 a 24 años ☐ 25 a 45 años ☒ 46 años en adelante

Sexo: ☒ Masculino ☐ Femenino

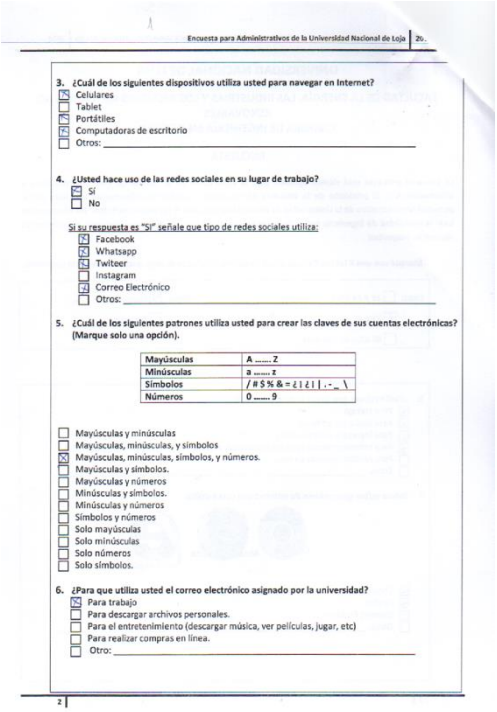
1. ¿Cuál es el uso que usted le da al Internet?
   - ☒ Para trabajo
   - ☐ Para descargar archivos
   - ☐ Para ingresar a redes sociales
   - ☒ Para entretenimiento (descargar/escuchar música, ver videos/películas, jugar, etc).
   - ☐ Para realizar compras en línea.
   - ☐ Otros: _____

2. Señale el/los navegadores de internet que usted utiliza.

   Chrome Mozilla Firefox I Explorer

   - ☒ Chrome
   - ☐ Firefox
   - ☐ Internet Explorer
   - ☐ Otros: _____

1



Encuesta para Administrativos de la Universidad Nacional de Loja | 20..

3. ¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?
   - ☒ Celulares
   - ☐ Tablet
   - ☒ Portátiles
   - ☒ Computadoras de escritorio
   - ☐ Otros: _____

4. ¿Usted hace uso de las redes sociales en su lugar de trabajo?
   - ☒ Si
   - ☐ No

   Si su respuesta es "Si" señale que tipo de redes sociales utiliza:
   - ☒ Facebook
   - ☒ Whatsapp
   - ☒ Twiteer
   - ☐ Instagram
   - ☒ Correo Electrónico
   - ☐ Otros: _____

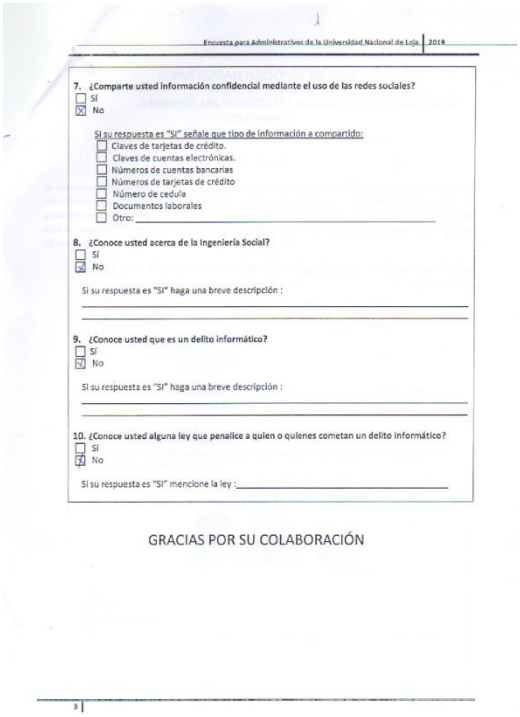
5. ¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).

Mayúsculas	A ..... Z
Minúsculas	a ..... z
Símbolos	/ # $ % & = ¿ ! ? ¡ | . - _ \
Números	0 9

   - ☐ Mayúsculas y minúsculas
   - ☐ Mayúsculas, minúsculas, y símbolos
   - ☒ Mayúsculas, minúsculas, símbolos, y números.
   - ☐ Mayúsculas y símbolos.
   - ☐ Mayúsculas y números
   - ☐ Minúsculas y símbolos.
   - ☐ Minúsculas y números
   - ☐ Símbolos y números
   - ☐ Solo mayúsculas
   - ☐ Solo minúsculas
   - ☐ Solo números
   - ☐ Solo símbolos.

6. ¿Para que utiliza usted el correo electrónico asignado por la universidad?
   - ☒ Para trabajo
   - ☐ Para descargar archivos personales.
   - ☐ Para el entretenimiento (descargar música, ver películas, jugar, etc)
   - ☐ Para realizar compras en línea.
   - ☐ Otro: _____

2



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

7. ¿Comparte usted información confidencial mediante el uso de las redes sociales?
   - ☐ SI
   - ☒ No

   Si su respuesta es "SI" señale que tipo de información a compartido:
   - ☐ Claves de tarjetas de crédito.
   - ☐ Claves de cuentas electrónicas.
   - ☐ Números de cuentas bancarias
   - ☐ Números de tarjetas de crédito
   - ☐ Número de cedula
   - ☐ Documentos laborales
   - ☐ Otro: _____

8. ¿Conoce usted acerca de la Ingeniería Social?
   - ☐ SI
   - ☒ No

   Si su respuesta es "SI" haga una breve descripción : _____

9. ¿Conoce usted que es un delito informático?
   - ☐ SI
   - ☒ No

   Si su respuesta es "SI" haga una breve descripción : _____

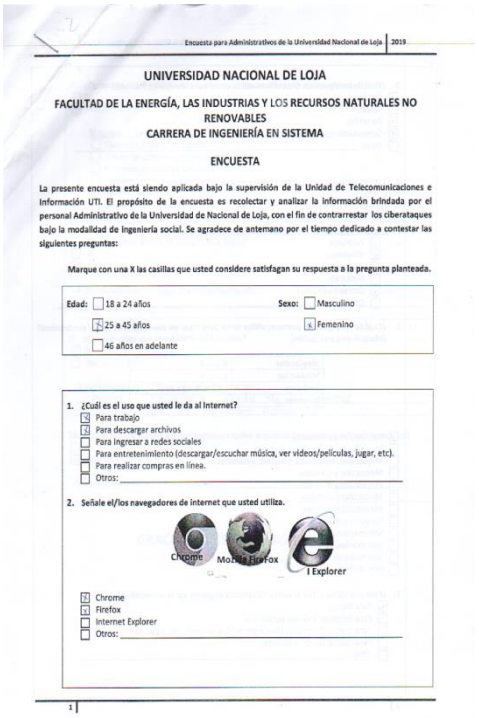
10. ¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?
    - ☐ SI
    - ☒ No

    Si su respuesta es "SI" mencione la ley : _____

GRACIAS POR SU COLABORACIÓN

3

- **Encuesta 002**



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMA

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e Información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de Ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

Edad: ☐ 18 a 24 años ☒ 25 a 45 años ☐ 46 años en adelante

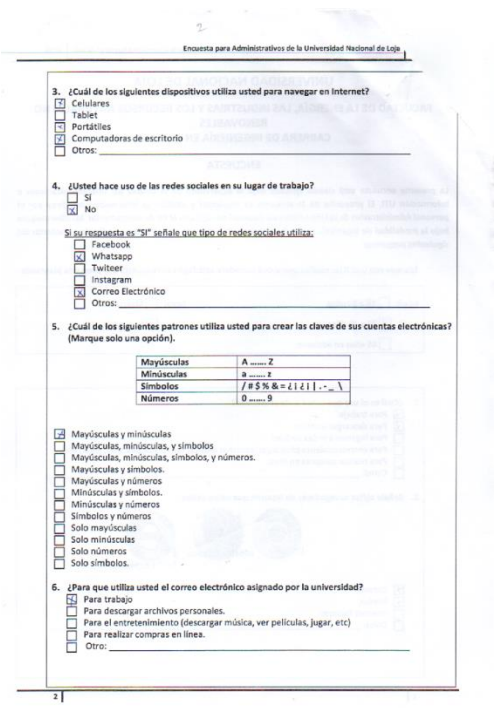
Sexo: ☐ Masculino ☒ Femenino

1. ¿Cuál es el uso que usted le da al Internet?
   - ☒ Para trabajo
   - ☒ Para descargar archivos
   - ☐ Para ingresar a redes sociales
   - ☐ Para entretenimiento (descargar/escuchar música, ver videos/películas, jugar, etc).
   - ☐ Para realizar compras en línea.
   - ☐ Otros: _____

2. Señale el/los navegadores de internet que usted utiliza.

   - ☒ Chrome
   - ☒ Firefox
   - ☐ Internet Explorer
   - ☐ Otros: _____

1



Encuesta para Administrativos de la Universidad Nacional de Loja

3. ¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?
   - ☒ Celulares
   - ☐ Tablet
   - ☒ Portátiles
   - ☒ Computadoras de escritorio
   - ☐ Otros: _____

4. ¿Usted hace uso de las redes sociales en su lugar de trabajo?
   - ☐ SI
   - ☒ No

   Si su respuesta es "SI" señale que tipo de redes sociales utiliza:
   - ☐ Facebook
   - ☒ Whatsapp
   - ☐ Twiteer
   - ☐ Instagram
   - ☒ Correo Electrónico
   - ☐ Otros: _____

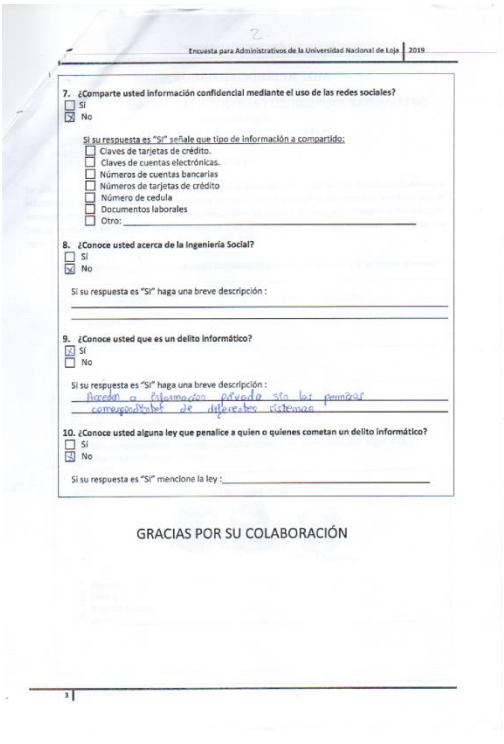
5. ¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).

Mayúsculas	A ..... Z
Minúsculas	a ..... z
Símbolos	/ # $ % & = ¿ ! ¿ ! | . - _ \
Números	0 9

   - ☒ Mayúsculas y minúsculas
   - ☐ Mayúsculas, minúsculas, y símbolos
   - ☐ Mayúsculas, minúsculas, símbolos, y números.
   - ☐ Mayúsculas y símbolos.
   - ☐ Mayúsculas y números
   - ☐ Minúsculas y símbolos.
   - ☐ Minúsculas y números
   - ☐ Símbolos y números
   - ☐ Solo mayúsculas
   - ☐ Solo minúsculas
   - ☐ Solo números
   - ☐ Solo símbolos.

6. ¿Para que utiliza usted el correo electrónico asignado por la universidad?
   - ☒ Para trabajo
   - ☐ Para descargar archivos personales.
   - ☐ Para el entretenimiento (descargar música, ver películas, jugar, etc)
   - ☐ Para realizar compras en línea.
   - ☐ Otro: _____

2



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

7. ¿Comparte usted información confidencial mediante el uso de las redes sociales?
   - ☐ SI
   - ☒ No

   Si su respuesta es "SI" señale que tipo de información a compartido:
   - ☐ Claves de tarjetas de crédito.
   - ☐ Claves de cuentas electrónicas.
   - ☐ Números de cuentas bancarias
   - ☐ Números de tarjetas de crédito
   - ☐ Número de cedula
   - ☐ Documentos laborales
   - ☐ Otro: _____

8. ¿Conoce usted acerca de la Ingeniería Social?
   - ☐ SI
   - ☒ No

   Si su respuesta es "SI" haga una breve descripción : _____

9. ¿Conoce usted que es un delito informático?
   - ☒ SI
   - ☐ No

   Si su respuesta es "SI" haga una breve descripción : Acceden a información privada sin los permisos correspondientes de diferentes sistemas

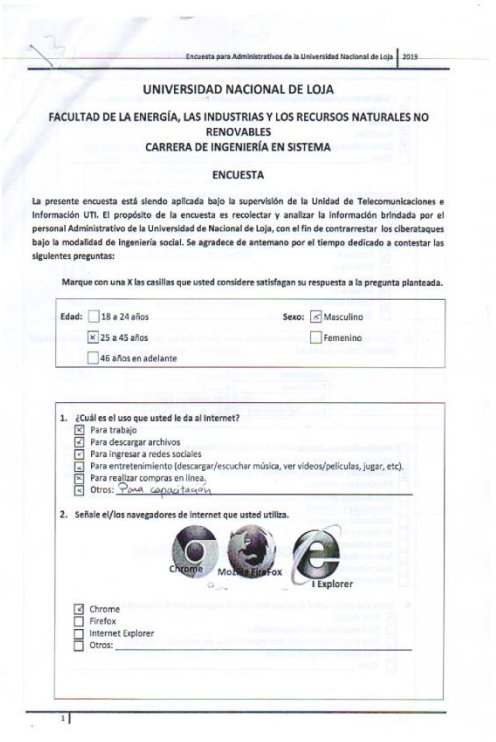
10. ¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?
    - ☐ SI
    - ☒ No

    Si su respuesta es "SI" menclone la ley : _____

GRACIAS POR SU COLABORACIÓN

3

- **Encuesta 003**



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMA

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e Información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

Edad: ☐ 18 a 24 años ☒ 25 a 45 años ☐ 46 años en adelante

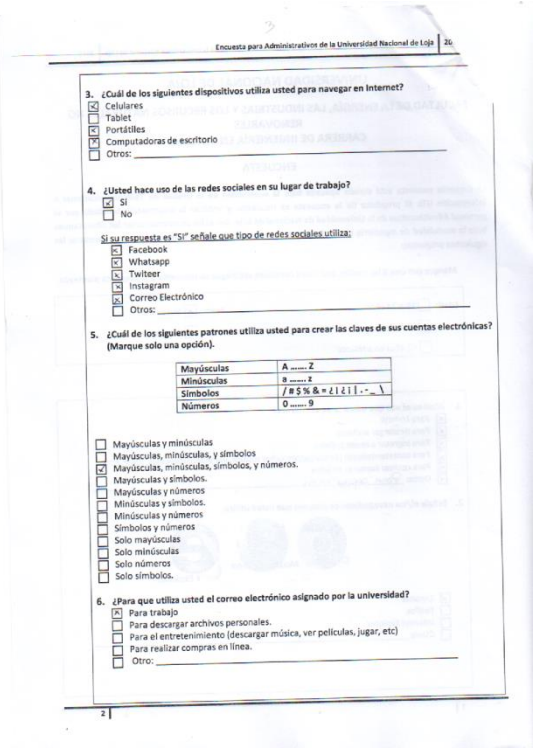
Sexo: ☒ Masculino ☐ Femenino

1. ¿Cuál es el uso que usted le da al Internet?
   - ☒ Para trabajo
   - ☒ Para descargar archivos
   - ☒ Para ingresar a redes sociales
   - ☒ Para entretenimiento (descargar/escuchar música, ver videos/películas, jugar, etc).
   - ☒ Para realizar compras en línea.
   - ☒ Otros: Para capacitación

2. Señale el/los navegadores de internet que usted utiliza.

   - ☒ Chrome
   - ☐ Firefox
   - ☐ Internet Explorer
   - ☐ Otros: _____

1



Encuesta para Administrativos de la Universidad Nacional de Loja | 20

3. ¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?
   - ☒ Celulares
   - ☐ Tablet
   - ☐ Portátiles
   - ☒ Computadoras de escritorio
   - ☐ Otros: _____

4. ¿Usted hace uso de las redes sociales en su lugar de trabajo?
   - ☒ Si
   - ☐ No

   Si su respuesta es "Si" señale que tipo de redes sociales utiliza:
   - ☒ Facebook
   - ☒ Whatsapp
   - ☒ Twiteer
   - ☒ Instagram
   - ☒ Correo Electrónico
   - ☐ Otros: _____

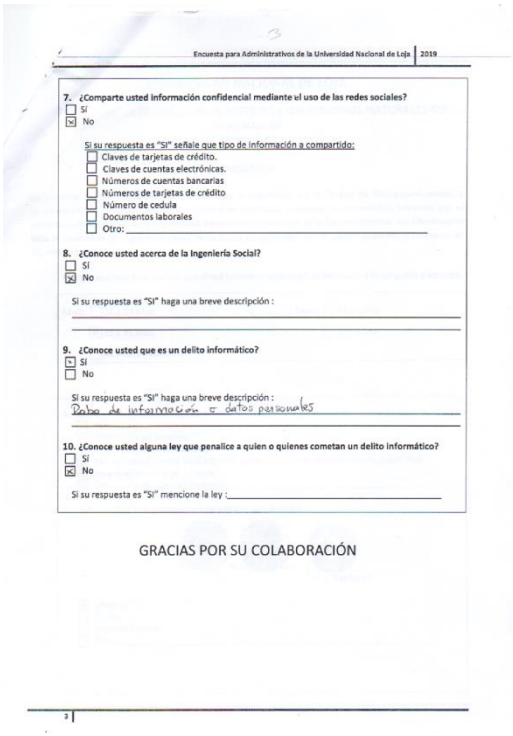
5. ¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).

Mayúsculas	A ..... Z
Minúsculas	a ..... z
Símbolos	/ # $ % & = ¿ ¡ ? | . - _ \
Números	0 9

   - ☐ Mayúsculas y minúsculas
   - ☐ Mayúsculas, minúsculas, y símbolos
   - ☒ Mayúsculas, minúsculas, símbolos, y números.
   - ☐ Mayúsculas y símbolos.
   - ☐ Mayúsculas y números
   - ☐ Minúsculas y símbolos.
   - ☐ Minúsculas y números
   - ☐ Símbolos y números
   - ☐ Solo mayúsculas
   - ☐ Solo minúsculas
   - ☐ Solo números
   - ☐ Solo símbolos.

6. ¿Para que utiliza usted el correo electrónico asignado por la universidad?
   - ☒ Para trabajo
   - ☐ Para descargar archivos personales.
   - ☐ Para el entretenimiento (descargar música, ver películas, jugar, etc)
   - ☐ Para realizar compras en línea.
   - ☐ Otro: _____

2



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

7. ¿Comparte usted información confidencial mediante el uso de las redes sociales?
   - ☐ Si
   - ☒ No

   Si su respuesta es "Si" señale que tipo de información a compartido:
   - ☐ Claves de tarjetas de crédito.
   - ☐ Claves de cuentas electrónicas.
   - ☐ Números de cuentas bancarias
   - ☐ Números de tarjetas de crédito
   - ☐ Número de cedula
   - ☐ Documentos laborales
   - ☐ Otro: _____

8. ¿Conoce usted acerca de la Ingeniería Social?
   - ☐ Si
   - ☒ No

   Si su respuesta es "Si" haga una breve descripción :

9. ¿Conoce usted que es un delito informático?
   - ☒ Si
   - ☐ No

   Si su respuesta es "Si" haga una breve descripción :
   Robo de información y datos personales

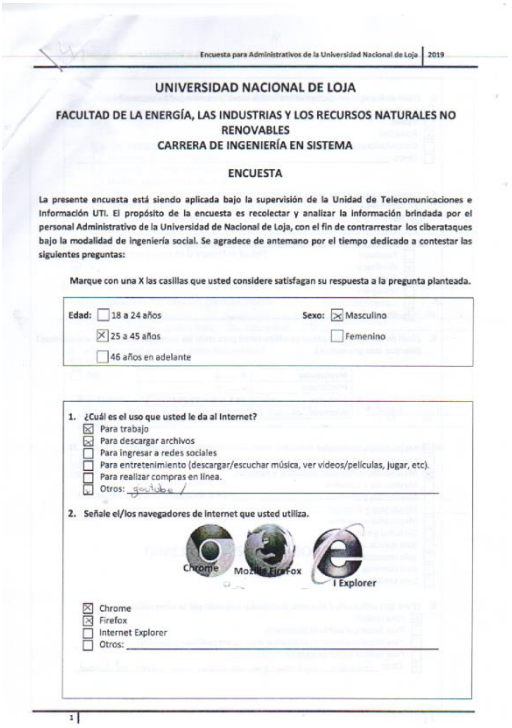
10. ¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?
    - ☐ Si
    - ☒ No

    Si su respuesta es "Si" mencione la ley : _____

GRACIAS POR SU COLABORACIÓN

3

- **Encuesta 004**



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES
CARRERA DE INGENIERÍA EN SISTEMA

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e Información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

Edad: ☐ 18 a 24 años ☒ 25 a 45 años ☐ 46 años en adelante

Sexo: ☒ Masculino ☐ Femenino

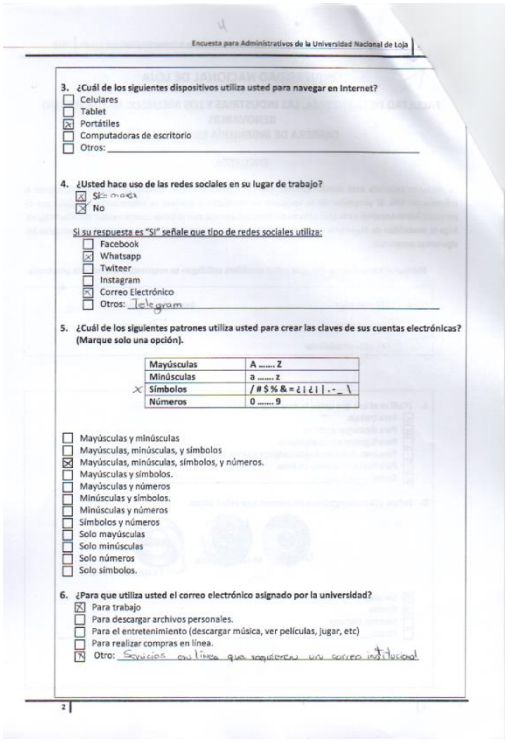
1. ¿Cuál es el uso que usted le da al Internet?
   - ☒ Para trabajo
   - ☒ Para descargar archivos
   - ☐ Para ingresar a redes sociales
   - ☐ Para entretenimiento (descargar/escuchar música, ver videos/películas, jugar, etc).
   - ☐ Para realizar compras en línea.
   - ☒ Otros: gestión /

2. Señale el/los navegadores de Internet que usted utiliza.

   Chrome Mozilla FireFox I Explorer

   - ☒ Chrome
   - ☒ Firefox
   - ☐ Internet Explorer
   - ☐ Otros: _____

1



Encuesta para Administrativos de la Universidad Nacional de Loja

3. ¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?
   - ☐ Celulares
   - ☐ Tablet
   - ☒ Portátiles
   - ☐ Computadoras de escritorio
   - ☐ Otros: _____

4. ¿Usted hace uso de las redes sociales en su lugar de trabajo?
   - ☒ Si a veces
   - ☒ No

   Si su respuesta es "Si" señale que tipo de redes sociales utiliza:
   - ☐ Facebook
   - ☒ Whatsapp
   - ☐ Twitter
   - ☐ Instagram
   - ☒ Correo Electrónico
   - ☐ Otros: Telegram

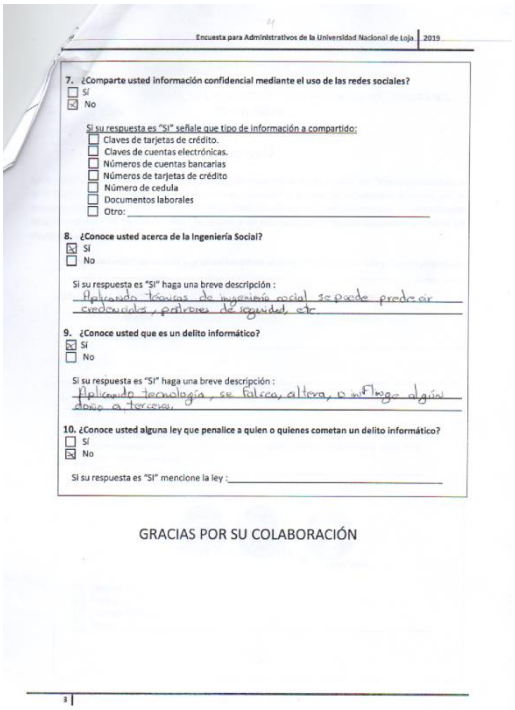
5. ¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).

	Mayúsculas	A ..... Z
	Minúsculas	a ..... z
X	Símbolos	/ # $ % & = ¿ ¡ ¿ ¡ | . - _ \
	Números	0 9

   - ☐ Mayúsculas y minúsculas
   - ☐ Mayúsculas, minúsculas, y símbolos
   - ☒ Mayúsculas, minúsculas, símbolos, y números.
   - ☐ Mayúsculas y símbolos.
   - ☐ Mayúsculas y números
   - ☐ Minúsculas y símbolos.
   - ☐ Minúsculas y números
   - ☐ Símbolos y números
   - ☐ Solo mayúsculas
   - ☐ Solo minúsculas
   - ☐ Solo números
   - ☐ Solo símbolos.

6. ¿Para que utiliza usted el correo electrónico asignado por la universidad?
   - ☒ Para trabajo
   - ☐ Para descargar archivos personales.
   - ☐ Para el entretenimiento (descargar música, ver películas, jugar, etc)
   - ☐ Para realizar compras en línea.
   - ☒ Otro: Servicios en línea que requieren un correo institucional

2



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

7. ¿Comparte usted información confidencial mediante el uso de las redes sociales?
   - ☐ Si
   - ☒ No

   Si su respuesta es "Si" señale que tipo de información a compartido:
   - ☐ Claves de tarjetas de crédito.
   - ☐ Claves de cuentas electrónicas.
   - ☐ Números de cuentas bancarias
   - ☐ Números de tarjetas de crédito
   - ☐ Número de cedula
   - ☐ Documentos laborales
   - ☐ Otro: _____

8. ¿Conoce usted acerca de la Ingeniería Social?
   - ☒ Si
   - ☐ No

   Si su respuesta es "Si" haga una breve descripción :
   Aplicando Técnicas de ingeniería social se puede predecir credenciales, políticas de seguridad, etc

9. ¿Conoce usted que es un delito informático?
   - ☒ Si
   - ☐ No

   Si su respuesta es "Si" haga una breve descripción :
   Aplicando tecnología, se falsea, altera, o influye alguna data a terceros.

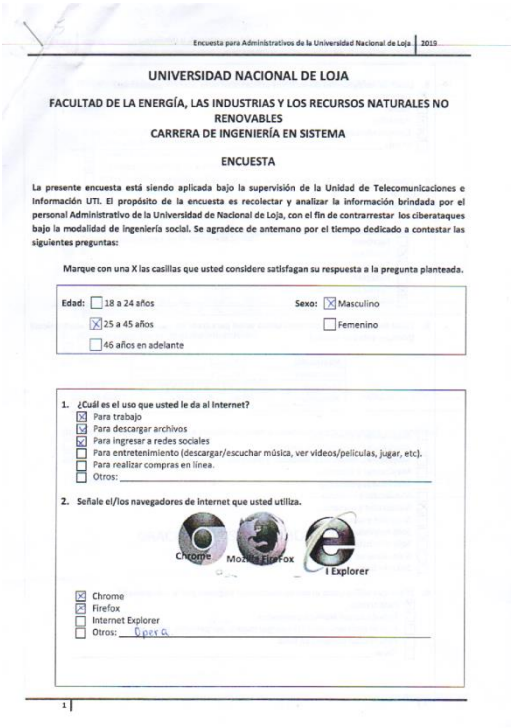
10. ¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?
    - ☐ Si
    - ☒ No

    Si su respuesta es "Si" mencione la ley : _____

GRACIAS POR SU COLABORACIÓN

3

- **Encuesta 005**



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMA

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e Información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

Edad: ☐ 18 a 24 años ☒ 25 a 45 años ☐ 46 años en adelante

Sexo: ☒ Masculino ☐ Femenino

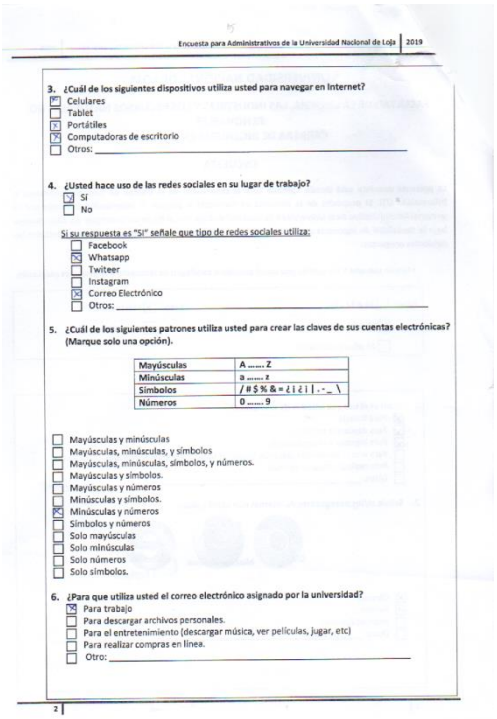
1. ¿Cuál es el uso que usted le da al Internet?
- ☒ Para trabajo
- ☒ Para descargar archivos
- ☒ Para ingresar a redes sociales
- ☐ Para entretenimiento (descargar/escuchar música, ver videos/películas, jugar, etc).
- ☐ Para realizar compras en línea.
- ☐ Otros: _____

2. Señale el/los navegadores de internet que usted utiliza.

Chrome Mozilla Firefox I Explorer

- ☒ Chrome
- ☒ Firefox
- ☐ Internet Explorer
- ☐ Otros: Opera

1



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

3. ¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?
- ☒ Celulares
- ☐ Tablet
- ☒ Portátiles
- ☒ Computadoras de escritorio
- ☐ Otros: _____

4. ¿Usted hace uso de las redes sociales en su lugar de trabajo?
- ☒ Sí
- ☐ No

Si su respuesta es "Sí" señale que tipo de redes sociales utiliza:
- ☐ Facebook
- ☒ Whatsapp
- ☐ Twiteer
- ☐ Instagram
- ☒ Correo Electrónico
- ☐ Otros: _____

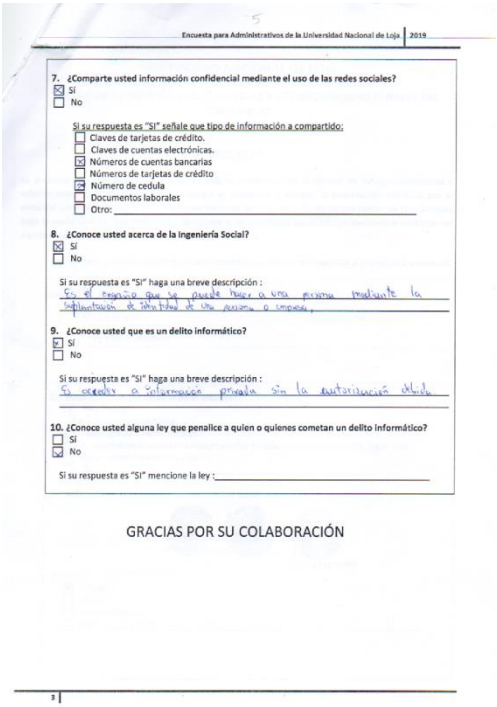
5. ¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).

Mayúsculas	A ..... Z
Minúsculas	a ..... z
Símbolos	/ # $ % & = ¿ ¡ ? | . - _ \
Números	0 9

- ☐ Mayúsculas y minúsculas
- ☐ Mayúsculas, minúsculas, y símbolos
- ☐ Mayúsculas, minúsculas, símbolos, y números.
- ☐ Mayúsculas y símbolos.
- ☐ Mayúsculas y números
- ☐ Minúsculas y símbolos.
- ☒ Minúsculas y números
- ☐ Símbolos y números
- ☐ Solo mayúsculas
- ☐ Solo minúsculas
- ☐ Solo números
- ☐ Solo símbolos.

6. ¿Para que utiliza usted el correo electrónico asignado por la universidad?
- ☒ Para trabajo
- ☐ Para descargar archivos personales.
- ☐ Para el entretenimiento (descargar música, ver películas, jugar, etc)
- ☐ Para realizar compras en línea.
- ☐ Otro: _____

2



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

7. ¿Comparte usted información confidencial mediante el uso de las redes sociales?
- ☒ Sí
- ☐ No

Si su respuesta es "Sí" señale que tipo de información a compartido:
- ☐ Claves de tarjetas de crédito.
- ☐ Claves de cuentas electrónicas.
- ☒ Números de cuentas bancarias
- ☐ Números de tarjetas de crédito
- ☒ Número de cedula
- ☐ Documentos laborales
- ☐ Otro: _____

8. ¿Conoce usted acerca de la Ingeniería Social?
- ☒ Sí
- ☐ No

Si su respuesta es "Sí" haga una breve descripción :
Es el engaño que se puede hacer a una persona mediante la información de interés de un equipo o empresa.

9. ¿Conoce usted que es un delito informático?
- ☒ Sí
- ☐ No

Si su respuesta es "Sí" haga una breve descripción :
Es acceder a información privada sin la autorización debida

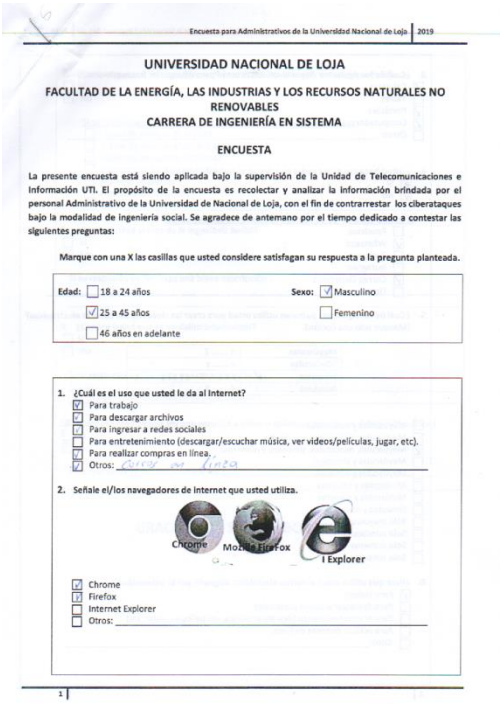
10. ¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?
- ☐ Sí
- ☒ No

Si su respuesta es "Sí" mencione la ley : _____

GRACIAS POR SU COLABORACIÓN

3

- **Encuesta 006**



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMA

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e Información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

Edad: ☐ 18 a 24 años ☑ 25 a 45 años ☐ 46 años en adelante

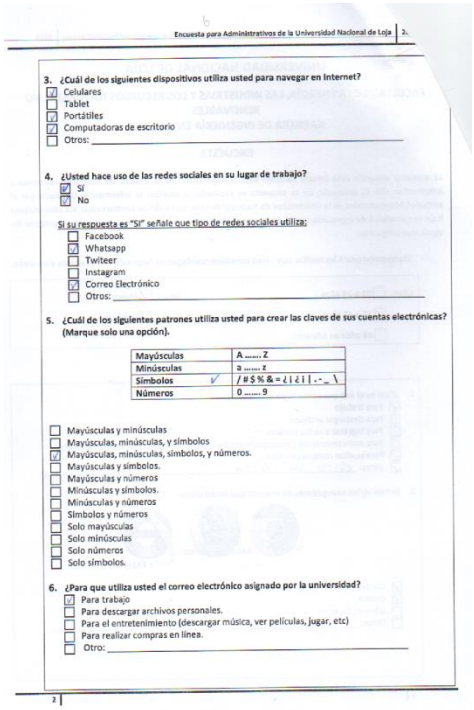
Sexo: ☑ Masculino ☐ Femenino

1. ¿Cuál es el uso que usted le da al Internet?
   - ☑ Para trabajo
   - ☑ Para descargar archivos
   - ☐ Para ingresar a redes sociales
   - ☐ Para entretenimiento (descargar/escuchar música, ver videos/películas, jugar, etc).
   - ☑ Para realizar compras en línea.
   - ☑ Otros: Citas en línea

2. Señale el/los navegadores de Internet que usted utiliza.

   - ☑ Chrome
   - ☑ Firefox
   - ☐ Internet Explorer
   - ☐ Otros: _____

1



Encuesta para Administrativos de la Universidad Nacional de Loja | 2.

3. ¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?
   - ☑ Celulares
   - ☐ Tablet
   - ☐ Portátiles
   - ☑ Computadoras de escritorio
   - ☐ Otros: _____

4. ¿Usted hace uso de las redes sociales en su lugar de trabajo?
   - ☑ Si
   - ☑ No

   Si su respuesta es "Si" señale que tipo de redes sociales utiliza:
   - ☐ Facebook
   - ☑ Whatsapp
   - ☐ Twiteer
   - ☐ Instagram
   - ☑ Correo Electrónico
   - ☐ Otros: _____

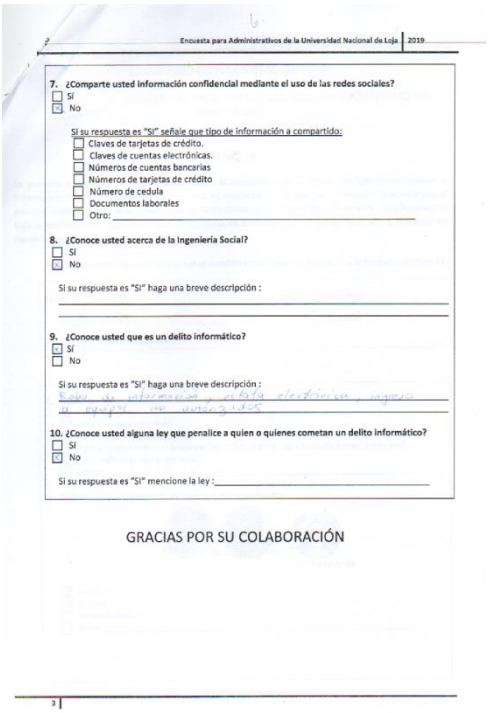
5. ¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).

Mayúsculas	A ..... Z
Minúsculas	a ..... z
Símbolos ✓	/ # $ % & = ¿ ! ¿ ! ! . - _ \
Números	0 9

   - ☐ Mayúsculas y minúsculas
   - ☐ Mayúsculas, minúsculas, y símbolos
   - ☑ Mayúsculas, minúsculas, símbolos, y números.
   - ☐ Mayúsculas y símbolos.
   - ☐ Mayúsculas y números
   - ☐ Minúsculas y símbolos.
   - ☐ Minúsculas y números
   - ☐ Símbolos y números
   - ☐ Solo mayúsculas
   - ☐ Solo minúsculas
   - ☐ Solo números
   - ☐ Solo símbolos.

6. ¿Para que utiliza usted el correo electrónico asignado por la universidad?
   - ☑ Para trabajo
   - ☐ Para descargar archivos personales.
   - ☐ Para el entretenimiento (descargar música, ver películas, jugar, etc)
   - ☐ Para realizar compras en línea.
   - ☐ Otro: _____

2



2 Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

7. ¿Comparte usted información confidencial mediante el uso de las redes sociales?
   - ☐ Si
   - ☒ No

   Si su respuesta es "Si" señale que tipo de información a compartido:
   - ☐ Claves de tarjetas de crédito.
   - ☐ Claves de cuentas electrónicas.
   - ☐ Números de cuentas bancarias
   - ☐ Números de tarjetas de crédito
   - ☐ Número de cedula
   - ☐ Documentos laborales
   - ☐ Otro: _____

8. ¿Conoce usted acerca de la Ingeniería Social?
   - ☐ Si
   - ☒ No

   Si su respuesta es "Si" haga una breve descripción :

9. ¿Conoce usted que es un delito informático?
   - ☐ Si
   - ☐ No

   Si su respuesta es "Si" haga una breve descripción :
   Robo de información y estafa electrónica, ingreso a equipos de manera ilegal

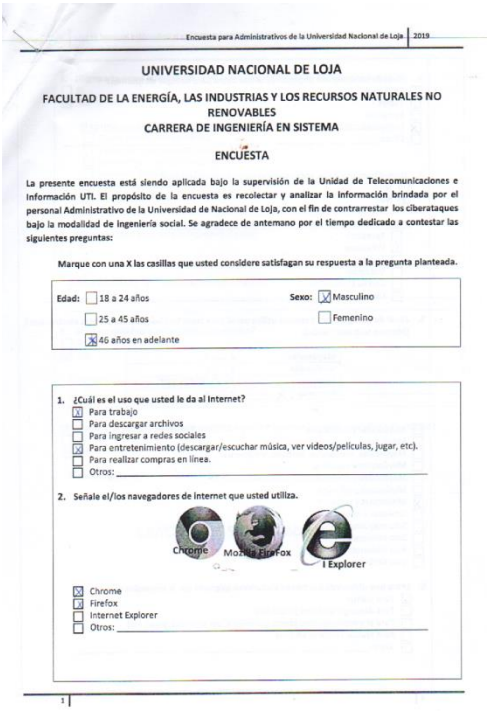
10. ¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?
    - ☐ Si
    - ☒ No

    Si su respuesta es "Si" mencione la ley :

GRACIAS POR SU COLABORACIÓN

3

- **Encuesta 007**



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMA

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e Información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de Ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

Edad: ☐ 18 a 24 años ☐ 25 a 45 años ☒ 46 años en adelante

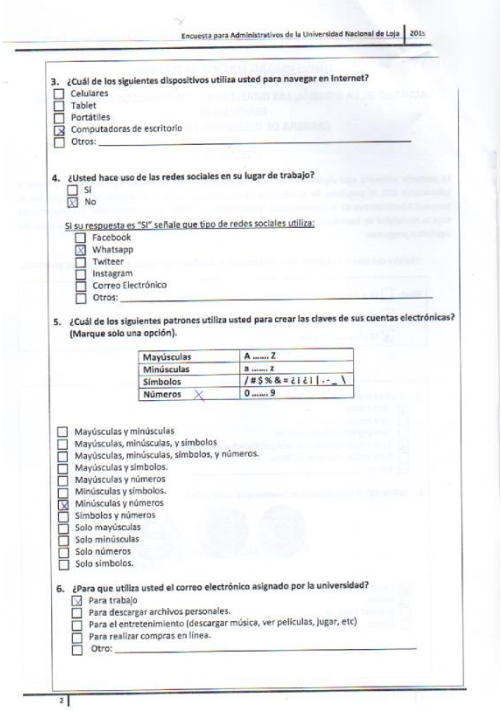
Sexo: ☒ Masculino ☐ Femenino

1. ¿Cuál es el uso que usted le da al Internet?
   - ☒ Para trabajo
   - ☐ Para descargar archivos
   - ☐ Para ingresar a redes sociales
   - ☒ Para entretenimiento (descargar/escuchar música, ver videos/películas, jugar, etc).
   - ☐ Para realizar compras en línea.
   - ☐ Otros: _____

2. Señale el/los navegadores de Internet que usted utiliza.

   - ☒ Chrome
   - ☒ Firefox
   - ☐ Internet Explorer
   - ☐ Otros: _____

1



Encuesta para Administrativos de la Universidad Nacional de Loja | 201

3. ¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?
   - ☐ Celulares
   - ☐ Tablet
   - ☐ Portátiles
   - ☒ Computadoras de escritorio
   - ☐ Otros: _____

4. ¿Usted hace uso de las redes sociales en su lugar de trabajo?
   - ☐ SI
   - ☒ No

   Si su respuesta es "SI" señale que tipo de redes sociales utiliza:
   - ☐ Facebook
   - ☒ Whatsapp
   - ☐ Twiteer
   - ☐ Instagram
   - ☐ Correo Electrónico
   - ☐ Otros: _____

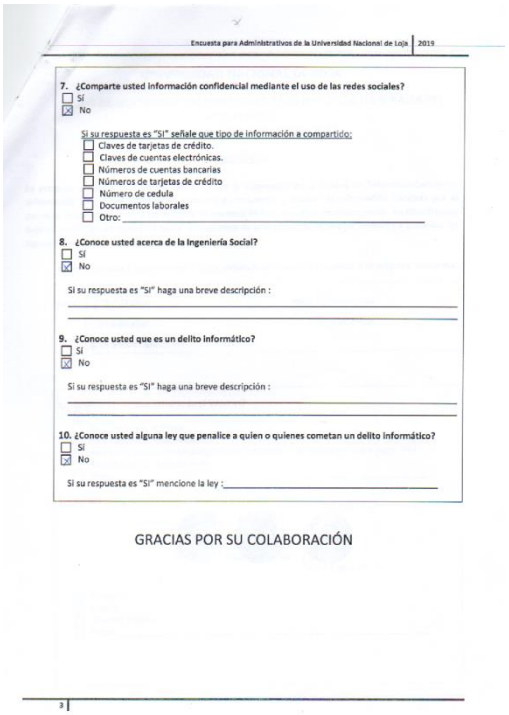
5. ¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).

Mayúsculas	A ..... Z
Minúsculas	a ..... z
Símbolos	/ # $ % & = ¿ ! ¿ ! | . - _ \
Números X	0 9

   - ☐ Mayúsculas y minúsculas
   - ☐ Mayúsculas, minúsculas, y símbolos
   - ☐ Mayúsculas, minúsculas, símbolos, y números.
   - ☐ Mayúsculas y símbolos.
   - ☐ Mayúsculas y números
   - ☐ Minúsculas y símbolos.
   - ☒ Minúsculas y números
   - ☐ Símbolos y números
   - ☐ Solo mayúsculas
   - ☐ Solo minúsculas
   - ☐ Solo números
   - ☐ Solo símbolos.

6. ¿Para que utiliza usted el correo electrónico asignado por la universidad?
   - ☒ Para trabajo
   - ☐ Para descargar archivos personales.
   - ☐ Para el entretenimiento (descargar música, ver películas, jugar, etc)
   - ☐ Para realizar compras en línea.
   - ☐ Otro: _____

2



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

7. ¿Comparte usted información confidencial mediante el uso de las redes sociales?
   - ☐ SI
   - ☒ No

   Si su respuesta es "SI" señale que tipo de información a compartido:
   - ☐ Claves de tarjetas de crédito.
   - ☐ Claves de cuentas electrónicas.
   - ☐ Números de cuentas bancarias
   - ☐ Números de tarjetas de crédito
   - ☐ Número de cedula
   - ☐ Documentos laborales
   - ☐ Otro: _____

8. ¿Conoce usted acerca de la Ingeniería Social?
   - ☐ SI
   - ☒ No

   Si su respuesta es "SI" haga una breve descripción : _____

9. ¿Conoce usted que es un delito informático?
   - ☐ SI
   - ☒ No

   Si su respuesta es "SI" haga una breve descripción : _____

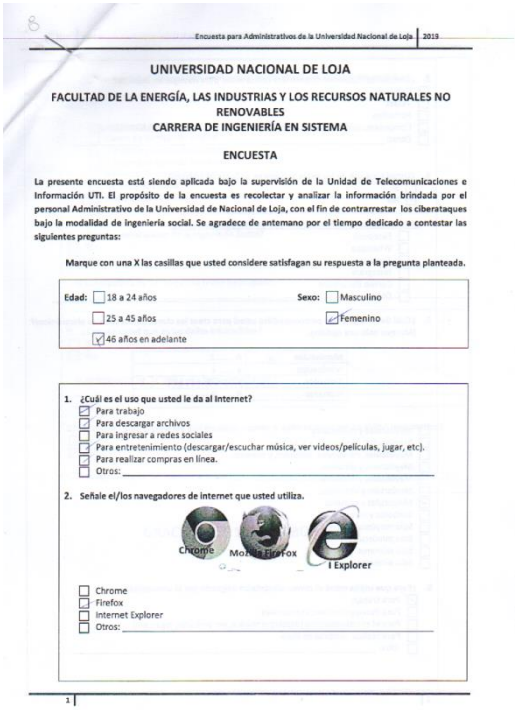
10. ¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?
    - ☐ SI
    - ☒ No

    Si su respuesta es "SI" mencione la ley : _____

GRACIAS POR SU COLABORACIÓN

3

- **Encuesta 008**



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMA

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e Información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

Edad: ☐ 18 a 24 años ☐ 25 a 45 años ☑ 46 años en adelante

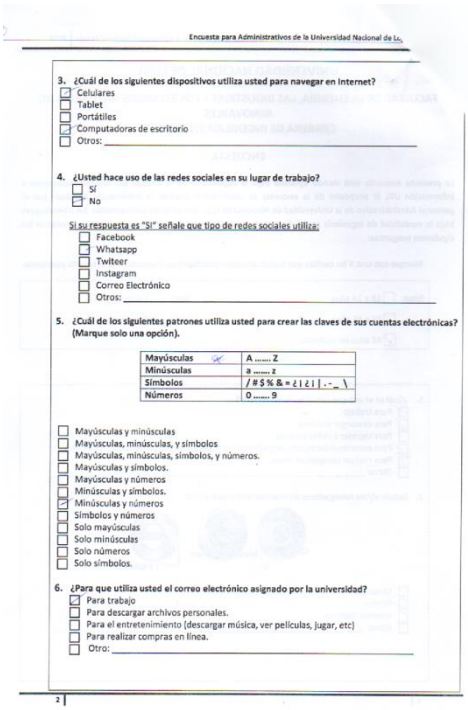
Sexo: ☐ Masculino ☑ Femenino

1. ¿Cuál es el uso que usted le da al Internet?
   - ☑ Para trabajo
   - ☑ Para descargar archivos
   - ☐ Para ingresar a redes sociales
   - ☑ Para entretenimiento (descargar/escuchar música, ver videos/películas, jugar, etc).
   - ☑ Para realizar compras en línea.
   - ☐ Otros: _____

2. Señale el/los navegadores de internet que usted utiliza.

   - ☐ Chrome
   - ☐ Firefox
   - ☐ Internet Explorer
   - ☐ Otros: _____

1



Encuesta para Administrativos de la Universidad Nacional de Lo...

3. ¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?
   - ☑ Celulares
   - ☐ Tablet
   - ☐ Portátiles
   - ☑ Computadoras de escritorio
   - ☐ Otros: _____

4. ¿Usted hace uso de las redes sociales en su lugar de trabajo?
   - ☐ Sí
   - ☑ No

   Si su respuesta es "Sí" señale que tipo de redes sociales utiliza:
   - ☐ Facebook
   - ☑ Whatsapp
   - ☐ Twiteer
   - ☐ Instagram
   - ☐ Correo Electrónico
   - ☐ Otros: _____

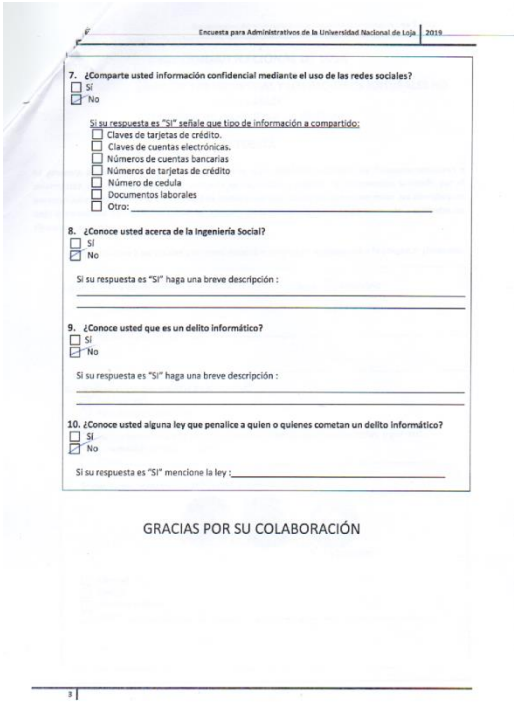
5. ¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).

Mayúsculas	A ..... Z
Minúsculas	a ..... z
Símbolos	/ # $ % & = ¿ ¡ ¿ ¡ | - - _ \
Números	0 9

   - ☐ Mayúsculas y minúsculas
   - ☐ Mayúsculas, minúsculas, y símbolos
   - ☐ Mayúsculas, minúsculas, símbolos, y números.
   - ☐ Mayúsculas y símbolos.
   - ☐ Mayúsculas y números
   - ☐ Minúsculas y símbolos.
   - ☑ Minúsculas y números
   - ☐ Símbolos y números
   - ☐ Solo mayúsculas
   - ☐ Solo minúsculas
   - ☐ Solo números
   - ☐ Solo símbolos.

6. ¿Para que utiliza usted el correo electrónico asignado por la universidad?
   - ☑ Para trabajo
   - ☐ Para descargar archivos personales.
   - ☐ Para el entretenimiento (descargar música, ver películas, jugar, etc)
   - ☐ Para realizar compras en línea.
   - ☐ Otro: _____

2



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

7. ¿Comparte usted información confidencial mediante el uso de las redes sociales?
   - ☐ Sí
   - ☑ No

   Si su respuesta es "Sí" señale que tipo de información a compartido:
   - ☐ Claves de tarjetas de crédito.
   - ☐ Claves de cuentas electrónicas.
   - ☐ Números de cuentas bancarias
   - ☐ Números de tarjetas de crédito
   - ☐ Número de cedula
   - ☐ Documentos laborales
   - ☐ Otro: _____

8. ¿Conoce usted acerca de la Ingeniería Social?
   - ☐ Sí
   - ☑ No

   Si su respuesta es "Sí" haga una breve descripción : _____

9. ¿Conoce usted que es un delito informático?
   - ☐ Sí
   - ☑ No

   Si su respuesta es "Sí" haga una breve descripción : _____

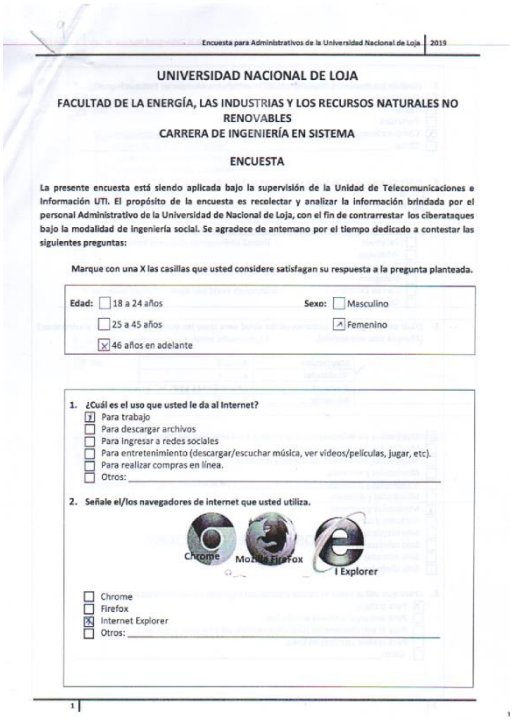
10. ¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?
    - ☐ Sí
    - ☑ No

    Si su respuesta es "Sí" mencione la ley : _____

GRACIAS POR SU COLABORACIÓN

3

- **Encuesta 009**



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMA

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e Información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

Edad: ☐ 18 a 24 años ☐ 25 a 45 años ☒ 46 años en adelante

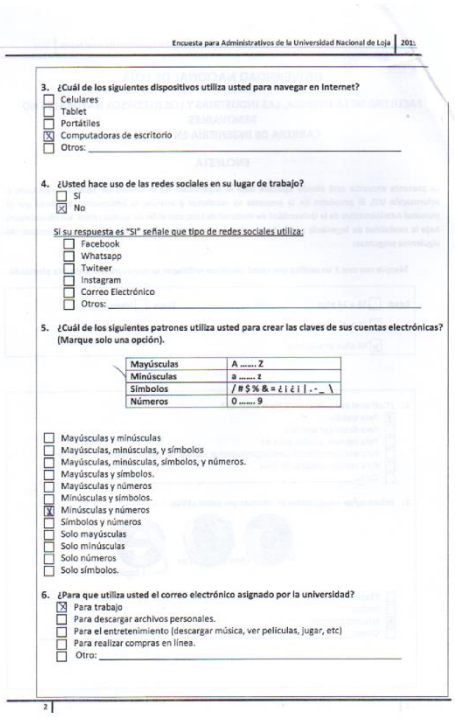
Sexo: ☐ Masculino ☒ Femenino

1. ¿Cuál es el uso que usted le da al Internet?
   - ☒ Para trabajo
   - ☐ Para descargar archivos
   - ☐ Para ingresar a redes sociales
   - ☐ Para entretenimiento (descargar/escuchar música, ver vídeos/películas, jugar, etc).
   - ☐ Para realizar compras en línea.
   - ☐ Otros: _____

2. Señale el/los navegadores de internet que usted utiliza.

   - ☐ Chrome
   - ☐ Firefox
   - ☒ Internet Explorer
   - ☐ Otros: _____

1



Encuesta para Administrativos de la Universidad Nacional de Loja | 201

3. ¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?
   - ☐ Celulares
   - ☐ Tablet
   - ☐ Portátiles
   - ☒ Computadoras de escritorio
   - ☐ Otros: _____

4. ¿Usted hace uso de las redes sociales en su lugar de trabajo?
   - ☐ Sí
   - ☒ No

   Si su respuesta es "SI" señale que tipo de redes sociales utiliza:
   - ☐ Facebook
   - ☐ Whatsapp
   - ☐ Twiteer
   - ☐ Instagram
   - ☐ Correo Electrónico
   - ☐ Otros: _____

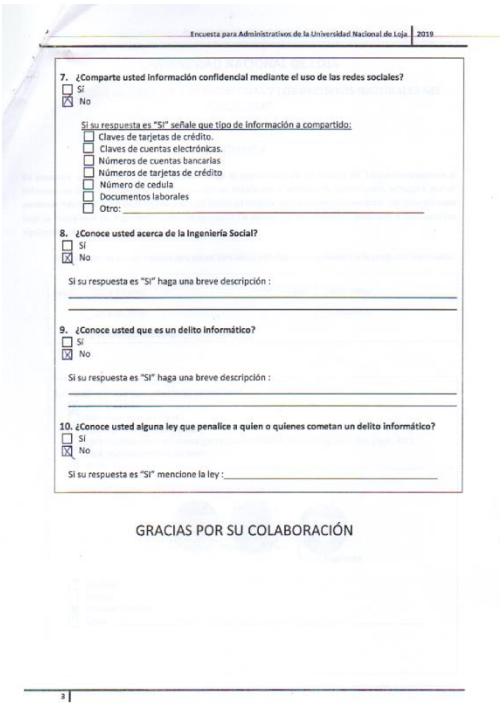
5. ¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).

Mayúsculas	A ..... Z
Minúsculas	a ..... z
Símbolos	/ # $ % & = ¿ ¡ ¿ ¡ | - _ \
Números	0 9

   - ☐ Mayúsculas y minúsculas
   - ☐ Mayúsculas, minúsculas, y símbolos
   - ☐ Mayúsculas, minúsculas, símbolos, y números.
   - ☐ Mayúsculas y símbolos.
   - ☐ Mayúsculas y números
   - ☐ Minúsculas y símbolos.
   - ☒ Minúsculas y números
   - ☐ Símbolos y números
   - ☐ Solo mayúsculas
   - ☐ Solo minúsculas
   - ☐ Solo números
   - ☐ Solo símbolos.

6. ¿Para que utiliza usted el correo electrónico asignado por la universidad?
   - ☒ Para trabajo
   - ☐ Para descargar archivos personales.
   - ☐ Para el entretenimiento (descargar música, ver películas, jugar, etc)
   - ☐ Para realizar compras en línea.
   - ☐ Otro: _____

2



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

7. ¿Comparte usted información confidencial mediante el uso de las redes sociales?
   - ☐ Sí
   - ☒ No

   Si su respuesta es "SI" señale que tipo de información a compartido:
   - ☐ Claves de tarjetas de crédito.
   - ☐ Claves de cuentas electrónicas.
   - ☐ Números de cuentas bancarias
   - ☐ Números de tarjetas de crédito
   - ☐ Número de cedula
   - ☐ Documentos laborales
   - ☐ Otro: _____

8. ¿Conoce usted acerca de la Ingeniería Social?
   - ☐ Sí
   - ☒ No

   Si su respuesta es "SI" haga una breve descripción : _____

9. ¿Conoce usted que es un delito informático?
   - ☐ Sí
   - ☒ No

   Si su respuesta es "SI" haga una breve descripción : _____

10. ¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?
    - ☐ Sí
    - ☒ No

    Si su respuesta es "SI" mencione la ley : _____

GRACIAS POR SU COLABORACIÓN

3

- **Encuesta 010**

Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES
CARRERA DE INGENIERÍA EN SISTEMA

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e Información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

Edad: ☐ 18 a 24 años ☐ 25 a 45 años ☒ 46 años en adelante

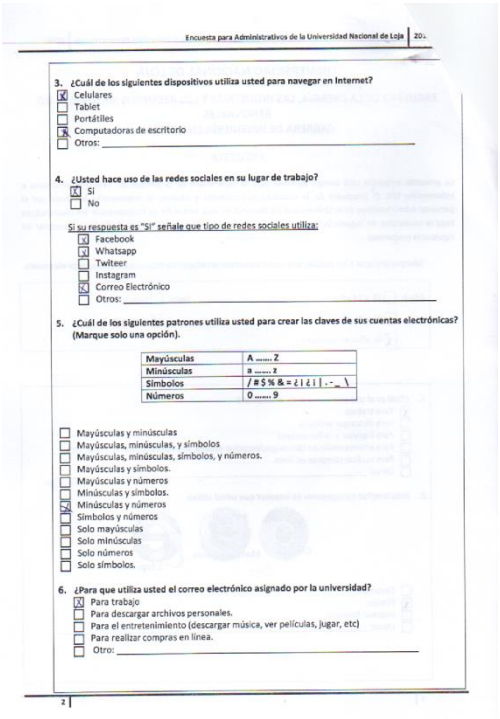
Sexo: ☐ Masculino ☒ Femenino

1. **¿Cuál es el uso que usted le da al Internet?**
   - ☒ Para trabajo
   - ☐ Para descargar archivos
   - ☐ Para ingresar a redes sociales
   - ☐ Para entretenimiento (descargar/escuchar música, ver videos/películas, jugar, etc).
   - ☐ Para realizar compras en línea.
   - ☐ Otros: _____
2. **Señale el/los navegadores de internet que usted utiliza.**

Chrome Mozilla FireFox I Explorer

- ☐ Chrome
- ☒ Firefox
- ☐ Internet Explorer
- ☐ Otros: _____

1



Encuesta para Administrativos de la Universidad Nacional de Loja | 20..

3. **¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?**
   - ☒ Celulares
   - ☐ Tablet
   - ☐ Portátiles
   - ☒ Computadoras de escritorio
   - ☐ Otros: _____
4. **¿Usted hace uso de las redes sociales en su lugar de trabajo?**
   - ☒ Si
   - ☐ No

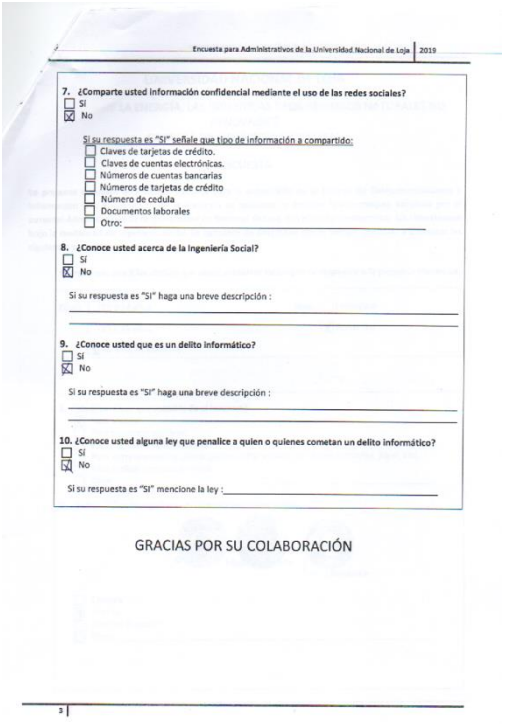
   Si su respuesta es "Si" señale que tipo de redes sociales utiliza:
   - ☒ Facebook
   - ☒ Whatsapp
   - ☐ Twiteer
   - ☐ Instagram
   - ☒ Correo Electrónico
   - ☐ Otros: _____
5. **¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).**

Mayúsculas	A ..... Z
Minúsculas	a ..... z
Símbolos	/ # $ % & = ¿ ! ¿ ! | . - _ \
Números	0 9

- ☐ Mayúsculas y minúsculas
- ☐ Mayúsculas, minúsculas, y símbolos
- ☐ Mayúsculas, minúsculas, símbolos, y números.
- ☐ Mayúsculas y símbolos.
- ☐ Mayúsculas y números
- ☐ Minúsculas y símbolos.
- ☒ Minúsculas y números
- ☐ Símbolos y números
- ☐ Solo mayúsculas
- ☐ Solo minúsculas
- ☐ Solo números
- ☐ Solo símbolos.

6. **¿Para que utiliza usted el correo electrónico asignado por la universidad?**
   - ☒ Para trabajo
   - ☐ Para descargar archivos personales.
   - ☐ Para el entretenimiento (descargar música, ver películas, jugar, etc)
   - ☐ Para realizar compras en línea.
   - ☐ Otro: _____

2



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

7. **¿Comparte usted información confidencial mediante el uso de las redes sociales?**
   - ☐ Si
   - ☒ No

   Si su respuesta es "Si" señale que tipo de información a compartido:
   - ☐ Claves de tarjetas de crédito.
   - ☐ Claves de cuentas electrónicas.
   - ☐ Números de cuentas bancarias
   - ☐ Números de tarjetas de crédito
   - ☐ Número de cedula
   - ☐ Documentos laborales
   - ☐ Otro: _____
8. **¿Conoce usted acerca de la Ingeniería Social?**
   - ☐ Si
   - ☒ No

   Si su respuesta es "Si" haga una breve descripción : _____
9. **¿Conoce usted que es un delito informático?**
   - ☐ Si
   - ☒ No

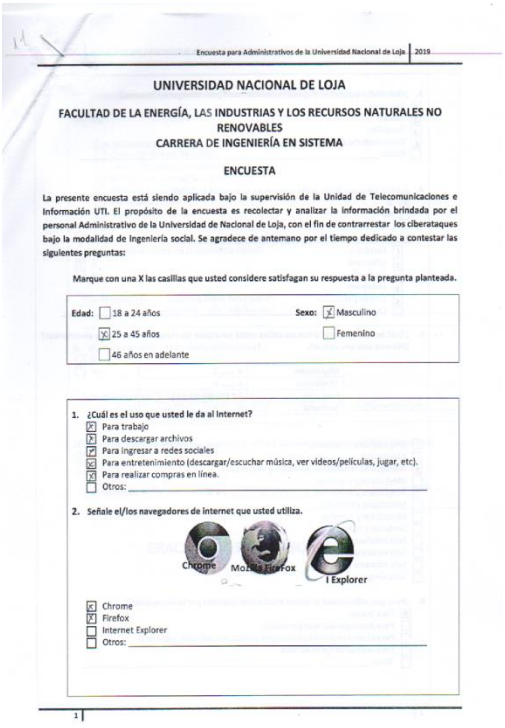
   Si su respuesta es "Si" haga una breve descripción : _____
10. **¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?**
    - ☐ Si
    - ☒ No

    Si su respuesta es "Si" mencione la ley : _____

GRACIAS POR SU COLABORACIÓN

3

- **Encuesta 011**



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMA

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e Información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de Ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

Edad: ☐ 18 a 24 años ☒ 25 a 45 años ☐ 46 años en adelante

Sexo: ☒ Masculino ☐ Femenino

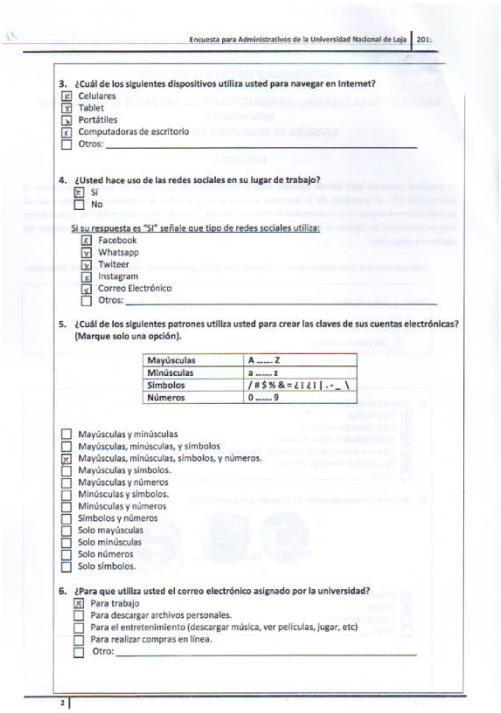
1. ¿Cuál es el uso que usted le da al Internet?
   - ☒ Para trabajo
   - ☒ Para descargar archivos
   - ☒ Para ingresar a redes sociales
   - ☒ Para entretenimiento (descargar/escuchar música, ver videos/películas, jugar, etc).
   - ☒ Para realizar compras en línea.
   - ☐ Otros: _____

2. Señale el/los navegadores de internet que usted utiliza.

Chrome Mozilla Firefox I Explorer

- ☒ Chrome
- ☒ Firefox
- ☐ Internet Explorer
- ☐ Otros: _____

1



Encuesta para Administrativos de la Universidad Nacional de Loja | 201

3. ¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?
   - ☒ Celulares
   - ☒ Tablet
   - ☒ Portátiles
   - ☒ Computadoras de escritorio
   - ☐ Otros: _____

4. ¿Usted hace uso de las redes sociales en su lugar de trabajo?
   - ☒ Si
   - ☐ No

Si su respuesta es "Si" señale que tipo de redes sociales utiliza:

- ☒ Facebook
- ☒ Whatsapp
- ☒ Twiteer
- ☒ Instagram
- ☒ Correo Electrónico
- ☐ Otros: _____

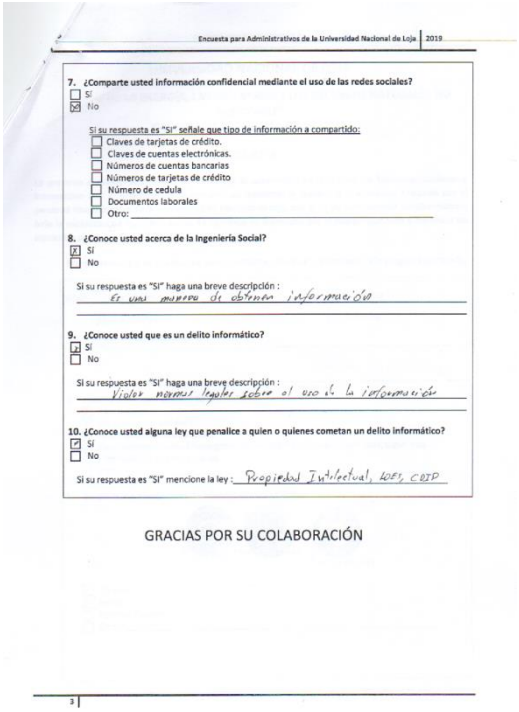
5. ¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).

Mayúsculas	A ..... Z
Minúsculas	a ..... z
Símbolos	/ # $ % & = ¿ ! ? ¡ | . - _ \
Números	0 9

- ☐ Mayúsculas y minúsculas
- ☐ Mayúsculas, minúsculas, y símbolos
- ☒ Mayúsculas, minúsculas, símbolos, y números.
- ☐ Mayúsculas y símbolos.
- ☐ Mayúsculas y números
- ☐ Minúsculas y símbolos.
- ☐ Minúsculas y números
- ☐ Símbolos y números
- ☐ Solo mayúsculas
- ☐ Solo minúsculas
- ☐ Solo números
- ☐ Solo símbolos.

6. ¿Para que utiliza usted el correo electrónico asignado por la universidad?
   - ☒ Para trabajo
   - ☐ Para descargar archivos personales.
   - ☐ Para el entretenimiento (descargar música, ver películas, jugar, etc)
   - ☐ Para realizar compras en línea.
   - ☐ Otro: _____

2



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

7. ¿Comparte usted información confidencial mediante el uso de las redes sociales?
   - ☐ Si
   - ☒ No

Si su respuesta es "Si" señale que tipo de información a compartido:

- ☐ Claves de tarjetas de crédito.
- ☐ Claves de cuentas electrónicas.
- ☐ Números de cuentas bancarias
- ☐ Números de tarjetas de crédito
- ☐ Número de cedula
- ☐ Documentos laborales
- ☐ Otro: _____

8. ¿Conoce usted acerca de la Ingeniería Social?
   - ☒ Si
   - ☐ No

Si su respuesta es "Si" haga una breve descripción :
Es una manera de obtener información

9. ¿Conoce usted que es un delito informático?
   - ☒ Si
   - ☐ No

Si su respuesta es "Si" haga una breve descripción :
Violar normas legales sobre el uso de la información

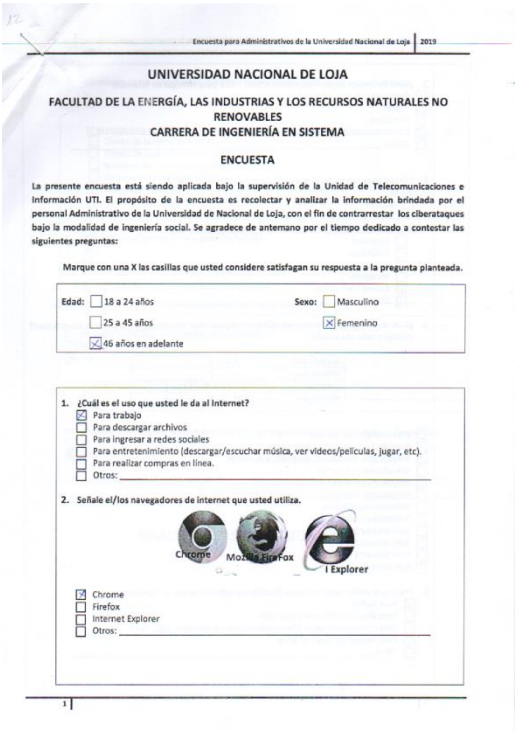
10. ¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?
    - ☒ Si
    - ☐ No

Si su respuesta es "Si" mencione la ley : Propiedad Intelectual, LOES, COIP

GRACIAS POR SU COLABORACIÓN

3

- **Encuesta 012**



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMA

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e Información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

Edad: ☐ 18 a 24 años ☐ 25 a 45 años ☒ 46 años en adelante

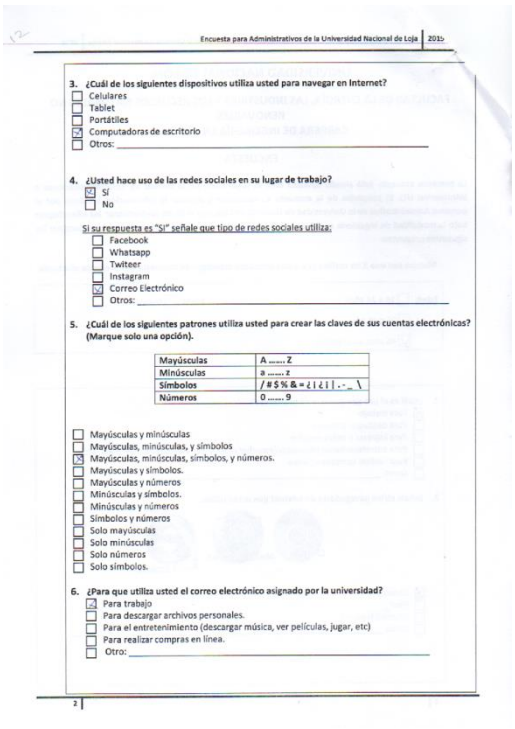
Sexo: ☐ Masculino ☒ Femenino

1. ¿Cuál es el uso que usted le da al Internet?
   - ☑ Para trabajo
   - ☐ Para descargar archivos
   - ☐ Para ingresar a redes sociales
   - ☐ Para entretenimiento (descargar/escuchar música, ver videos/películas, jugar, etc).
   - ☐ Para realizar compras en línea.
   - ☐ Otros: _____

2. Señale el/los navegadores de internet que usted utiliza.

   - ☑ Chrome
   - ☐ Firefox
   - ☐ Internet Explorer
   - ☐ Otros: _____

1



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

3. ¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?
   - ☐ Celulares
   - ☐ Tablet
   - ☐ Portátiles
   - ☑ Computadoras de escritorio
   - ☐ Otros: _____

4. ¿Usted hace uso de las redes sociales en su lugar de trabajo?
   - ☑ Sí
   - ☐ No

   Si su respuesta es "Si" señale que tipo de redes sociales utiliza:
   - ☐ Facebook
   - ☐ Whatsapp
   - ☐ Twiteer
   - ☐ Instagram
   - ☑ Correo Electrónico
   - ☐ Otros: _____

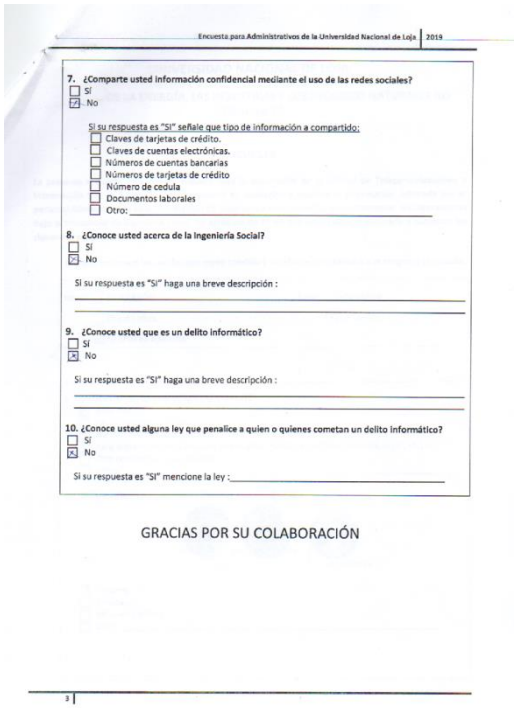
5. ¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).

Mayúsculas	A ..... Z
Minúsculas	a ..... z
Símbolos	/ # $ % & = ¿ ¡ ¿ ¡ . - _ \
Números	0 9

   - ☐ Mayúsculas y minúsculas
   - ☐ Mayúsculas, minúsculas, y símbolos
   - ☒ Mayúsculas, minúsculas, símbolos, y números.
   - ☐ Mayúsculas y símbolos.
   - ☐ Mayúsculas y números
   - ☐ Minúsculas y símbolos.
   - ☐ Minúsculas y números
   - ☐ Símbolos y números
   - ☐ Solo mayúsculas
   - ☐ Solo minúsculas
   - ☐ Solo números
   - ☐ Solo símbolos.

6. ¿Para que utiliza usted el correo electrónico asignado por la universidad?
   - ☑ Para trabajo
   - ☐ Para descargar archivos personales.
   - ☐ Para el entretenimiento (descargar música, ver películas, jugar, etc)
   - ☐ Para realizar compras en línea.
   - ☐ Otro: _____

2



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

7. ¿Comparte usted información confidencial mediante el uso de las redes sociales?
   - ☐ Sí
   - ☑ No

   Si su respuesta es "Si" señale que tipo de información a compartido:
   - ☐ Claves de tarjetas de crédito.
   - ☐ Claves de cuentas electrónicas.
   - ☐ Números de cuentas bancarias
   - ☐ Números de tarjetas de crédito
   - ☐ Número de cedula
   - ☐ Documentos laborales
   - ☐ Otro: _____

8. ¿Conoce usted acerca de la Ingeniería Social?
   - ☐ Sí
   - ☒ No

   Si su respuesta es "Si" haga una breve descripción : _____

9. ¿Conoce usted que es un delito informático?
   - ☐ Sí
   - ☒ No

   Si su respuesta es "Si" haga una breve descripción : _____

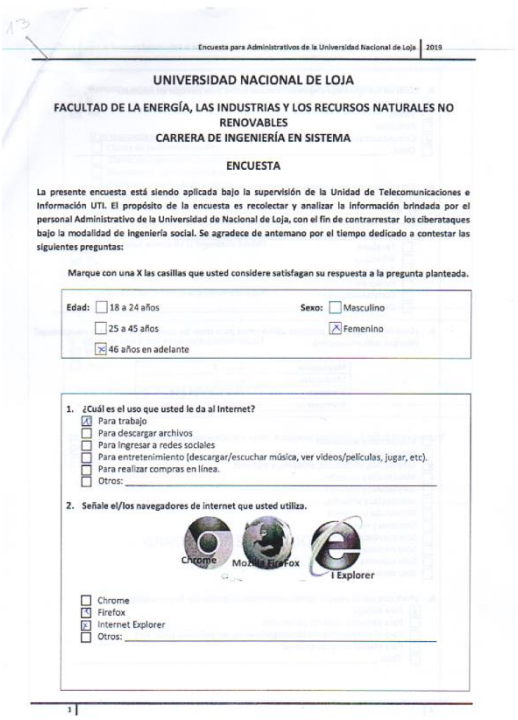
10. ¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?
    - ☐ Sí
    - ☒ No

    Si su respuesta es "Si" mencione la ley : _____

GRACIAS POR SU COLABORACIÓN

3

- **Encuesta 013**



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMA

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e Información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de Ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

Edad: ☐ 18 a 24 años ☐ 25 a 45 años ☒ 46 años en adelante

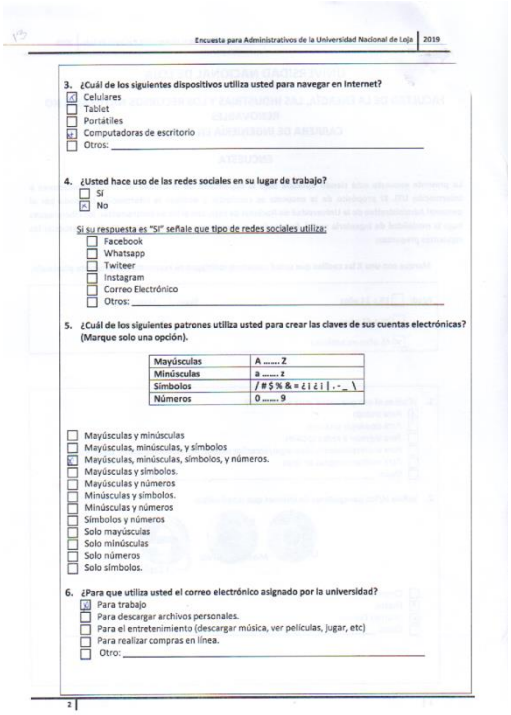
Sexo: ☐ Masculino ☒ Femenino

1. ¿Cuál es el uso que usted le da al Internet?
   - ☒ Para trabajo
   - ☐ Para descargar archivos
   - ☐ Para ingresar a redes sociales
   - ☐ Para entretenimiento (descargar/escuchar música, ver videos/películas, jugar, etc).
   - ☐ Para realizar compras en línea.
   - ☐ Otros: _____

2. Señale el/los navegadores de internet que usted utiliza.

   - ☐ Chrome
   - ☒ Firefox
   - ☒ Internet Explorer
   - ☐ Otros: _____

1



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

3. ¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?
   - ☒ Celulares
   - ☐ Tablet
   - ☐ Portátiles
   - ☒ Computadoras de escritorio
   - ☐ Otros: _____

4. ¿Usted hace uso de las redes sociales en su lugar de trabajo?
   - ☐ Si
   - ☒ No

   Si su respuesta es "Si" señale que tipo de redes sociales utiliza:
   - ☐ Facebook
   - ☐ Whatsapp
   - ☐ Twiteer
   - ☐ Instagram
   - ☐ Correo Electrónico
   - ☐ Otros: _____

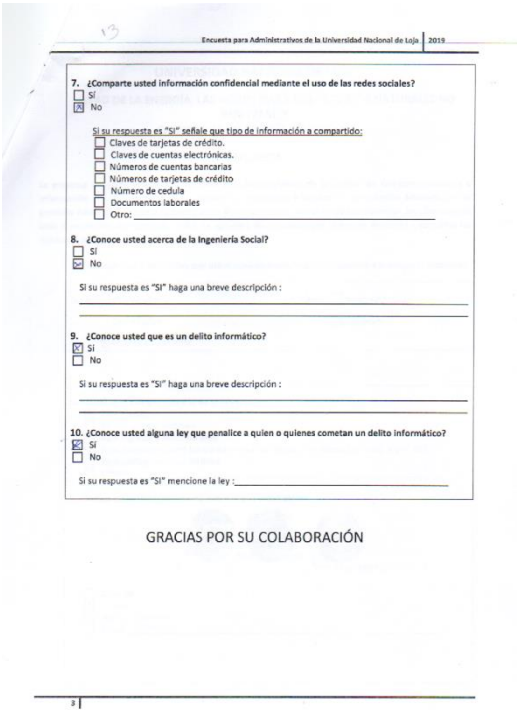
5. ¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).

Mayúsculas	A ..... Z
Minúsculas	a ..... z
Símbolos	/ # $ % & = ¿ ! ¿ ! | . - _ \
Números	0 9

   - ☐ Mayúsculas y minúsculas
   - ☐ Mayúsculas, minúsculas, y símbolos
   - ☒ Mayúsculas, minúsculas, símbolos, y números.
   - ☐ Mayúsculas y símbolos.
   - ☐ Mayúsculas y números
   - ☐ Minúsculas y símbolos.
   - ☐ Minúsculas y números
   - ☐ Símbolos y números
   - ☐ Solo mayúsculas
   - ☐ Solo minúsculas
   - ☐ Solo números
   - ☐ Solo símbolos.

6. ¿Para que utiliza usted el correo electrónico asignado por la universidad?
   - ☒ Para trabajo
   - ☐ Para descargar archivos personales.
   - ☐ Para el entretenimiento (descargar música, ver películas, jugar, etc)
   - ☐ Para realizar compras en línea.
   - ☐ Otro: _____

2



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

7. ¿Comparte usted información confidencial mediante el uso de las redes sociales?
   - ☐ Si
   - ☒ No

   Si su respuesta es "Si" señale que tipo de información a compartido:
   - ☐ Claves de tarjetas de crédito.
   - ☐ Claves de cuentas electrónicas.
   - ☐ Números de cuentas bancarias
   - ☐ Números de tarjetas de crédito
   - ☐ Número de cedula
   - ☐ Documentos laborales
   - ☐ Otro: _____

8. ¿Conoce usted acerca de la Ingeniería Social?
   - ☐ Si
   - ☒ No

   Si su respuesta es "Si" haga una breve descripción :

   _____

   _____

9. ¿Conoce usted que es un delito informático?
   - ☒ Si
   - ☐ No

   Si su respuesta es "Si" haga una breve descripción :

   _____

   _____

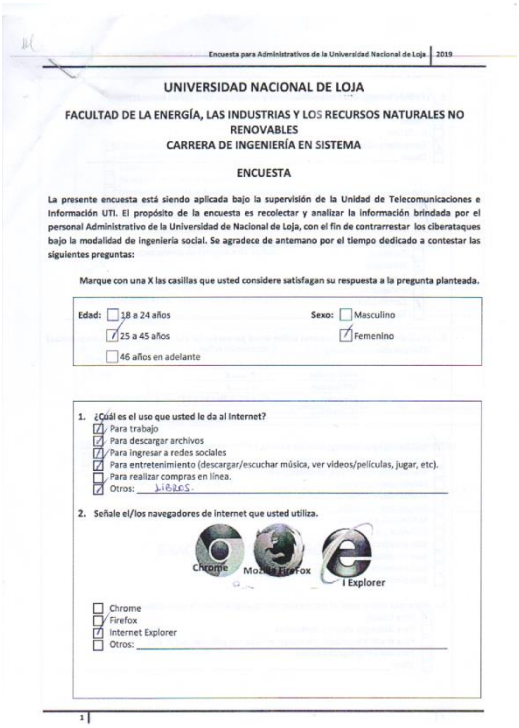
10. ¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?
    - ☒ Si
    - ☐ No

    Si su respuesta es "Si" mencione la ley : _____

GRACIAS POR SU COLABORACIÓN

3

- **Encuesta 014**



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMA

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e Información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

Edad: [ ] 18 a 24 años [X] 25 a 45 años [ ] 46 años en adelante

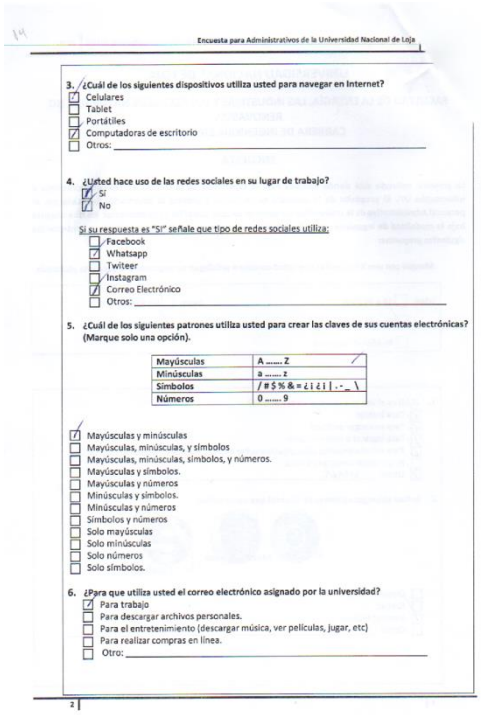
Sexo: [ ] Masculino [X] Femenino

1. ¿Cuál es el uso que usted le da al Internet?
   - [X] Para trabajo
   - [X] Para descargar archivos
   - [X] Para ingresar a redes sociales
   - [X] Para entretenimiento (descargar/escuchar música, ver videos/películas, jugar, etc).
   - [ ] Para realizar compras en línea.
   - [X] Otros: LIBROS.
2. Señale el/los navegadores de internet que usted utiliza.

   Chrome Mozilla Firefox I Explorer

   - [ ] Chrome
   - [X] Firefox
   - [X] Internet Explorer
   - [ ] Otros: _____

1



Encuesta para Administrativos de la Universidad Nacional de Loja

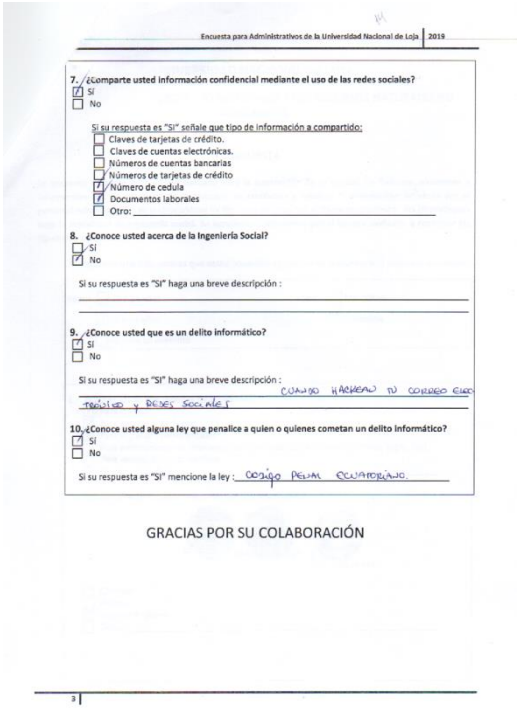
3. ¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?
   - [X] Celulares
   - [ ] Tablet
   - [ ] Portátiles
   - [X] Computadoras de escritorio
   - [ ] Otros: _____
4. ¿Usted hace uso de las redes sociales en su lugar de trabajo?
   - [X] Si
   - [X] No

   Si su respuesta es "Si" señale que tipo de redes sociales utiliza:
   - [ ] Facebook
   - [X] Whatsapp
   - [ ] Twiteer
   - [X] Instagram
   - [X] Correo Electrónico
   - [ ] Otros: _____
5. ¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).

Mayúsculas	A ..... Z
Minúsculas	a ..... z
Símbolos	/ # $ % & = ¿ ¡ ¦ . - _ \
Números	0 9

   - [X] Mayúsculas y minúsculas
   - [ ] Mayúsculas, minúsculas, y símbolos
   - [ ] Mayúsculas, minúsculas, símbolos, y números.
   - [ ] Mayúsculas y símbolos.
   - [ ] Mayúsculas y números
   - [ ] Minúsculas y símbolos.
   - [ ] Minúsculas y números
   - [ ] Símbolos y números
   - [ ] Solo mayúsculas
   - [ ] Solo minúsculas
   - [ ] Solo números
   - [ ] Solo símbolos.
6. ¿Para que utiliza usted el correo electrónico asignado por la universidad?
   - [X] Para trabajo
   - [ ] Para descargar archivos personales.
   - [ ] Para el entretenimiento (descargar música, ver películas, jugar, etc)
   - [ ] Para realizar compras en línea.
   - [ ] Otro: _____

2



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

7. ¿Comparte usted información confidencial mediante el uso de las redes sociales?
   - [X] Si
   - [ ] No

   Si su respuesta es "Si" señale que tipo de información a compartido:
   - [ ] Claves de tarjetas de crédito.
   - [ ] Claves de cuentas electrónicas.
   - [ ] Números de cuentas bancarias
   - [ ] Números de tarjetas de crédito
   - [X] Número de cedula
   - [X] Documentos laborales
   - [ ] Otro: _____
8. ¿Conoce usted acerca de la Ingeniería Social?
   - [ ] Si
   - [X] No

   Si su respuesta es "Si" haga una breve descripción :
   _____
   _____
9. ¿Conoce usted que es un delito informático?
   - [X] Si
   - [ ] No

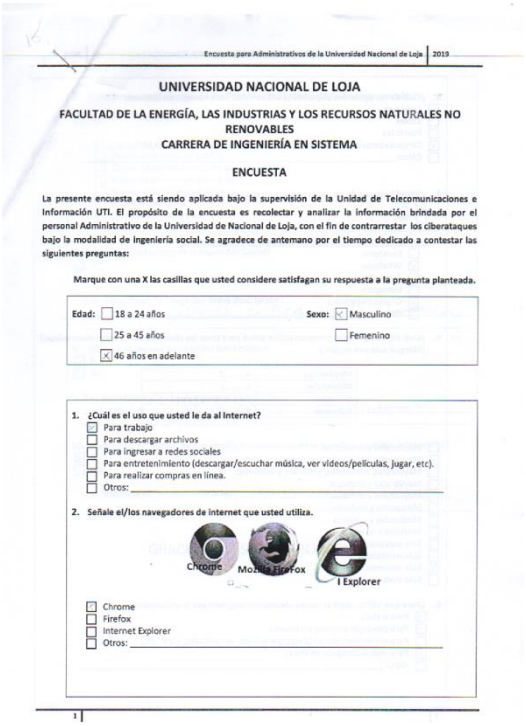
   Si su respuesta es "Si" haga una breve descripción : CUANDO HACKEAN TU CORREO ELEC
   TRÓNICO Y REDES SOCIALES
10. ¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?
    - [X] Si
    - [ ] No

    Si su respuesta es "Si" mencione la ley : CODIGO PENAL ECUATORIANO.

GRACIAS POR SU COLABORACIÓN

3

- **Encuesta 015**



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMA

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e Información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

Edad: ☐ 18 a 24 años ☐ 25 a 45 años ☒ 46 años en adelante

Sexo: ☑ Masculino ☐ Femenino

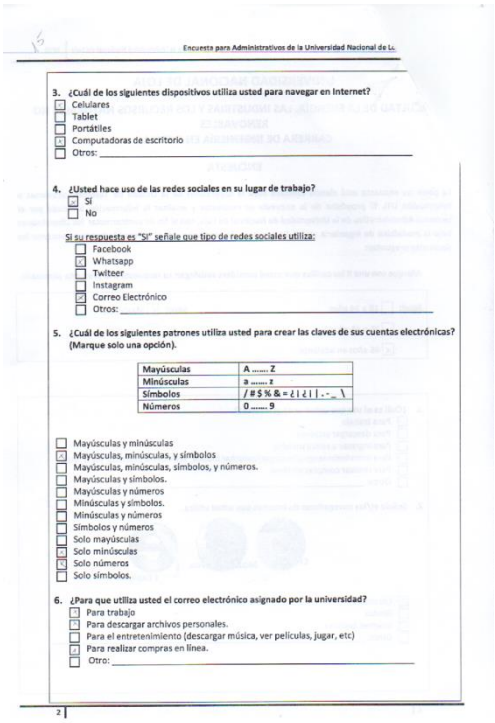
1. ¿Cuál es el uso que usted le da al Internet?
   - ☑ Para trabajo
   - ☐ Para descargar archivos
   - ☐ Para ingresar a redes sociales
   - ☐ Para entretenimiento (descargar/escuchar música, ver videos/peliculas, jugar, etc).
   - ☐ Para realizar compras en línea.
   - ☐ Otros: _____

2. Señale el/los navegadores de internet que usted utiliza.

   Chrome Mozilla Firefox I Explorer

   - ☑ Chrome
   - ☐ Firefox
   - ☐ Internet Explorer
   - ☐ Otros: _____

1



Encuesta para Administrativos de la Universidad Nacional de Lo

3. ¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?
   - ☐ Celulares
   - ☐ Tablet
   - ☐ Portátiles
   - ☑ Computadoras de escritorio
   - ☐ Otros: _____

4. ¿Usted hace uso de las redes sociales en su lugar de trabajo?
   - ☑ Si
   - ☐ No

   Si su respuesta es "Si" señale que tipo de redes sociales utiliza:
   - ☐ Facebook
   - ☒ Whatsapp
   - ☐ Twiteer
   - ☐ Instagram
   - ☑ Correo Electrónico
   - ☐ Otros: _____

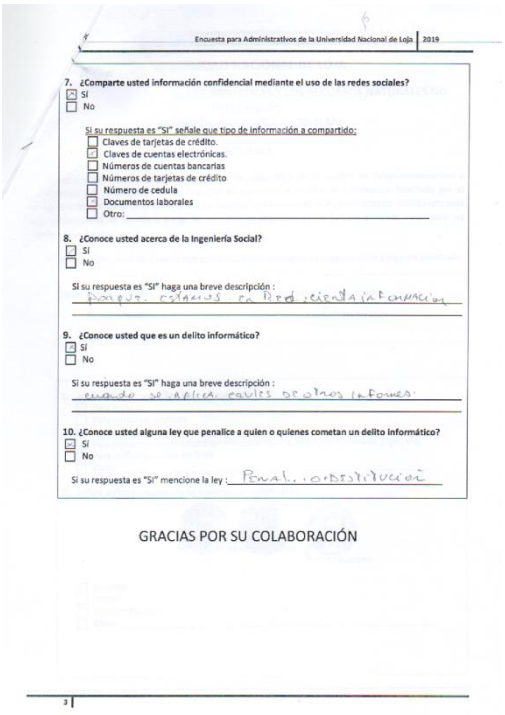
5. ¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).

Mayúsculas	A ..... Z
Minúsculas	a ..... z
Símbolos	/ # $ % & = ¿ ¡ ¿ | . - _ \
Números	0 9

   - ☐ Mayúsculas y minúsculas
   - ☑ Mayúsculas, minúsculas, y símbolos
   - ☐ Mayúsculas, minúsculas, símbolos, y números.
   - ☐ Mayúsculas y símbolos.
   - ☐ Mayúsculas y números
   - ☐ Minúsculas y símbolos.
   - ☐ Minúsculas y números
   - ☐ Símbolos y números
   - ☐ Solo mayúsculas
   - ☑ Solo minúsculas
   - ☐ Solo números
   - ☐ Solo símbolos.

6. ¿Para que utiliza usted el correo electrónico asignado por la universidad?
   - ☐ Para trabajo
   - ☐ Para descargar archivos personales.
   - ☐ Para el entretenimiento (descargar música, ver películas, jugar, etc)
   - ☑ Para realizar compras en línea.
   - ☐ Otro: _____

2



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

7. ¿Comparte usted información confidencial mediante el uso de las redes sociales?
   - ☑ Si
   - ☐ No

   Si su respuesta es "Si" señale que tipo de información a compartido:
   - ☐ Claves de tarjetas de crédito.
   - ☑ Claves de cuentas electrónicas.
   - ☐ Números de cuentas bancarias
   - ☐ Números de tarjetas de crédito
   - ☐ Número de cedula
   - ☑ Documentos laborales
   - ☐ Otro: _____

8. ¿Conoce usted acerca de la Ingeniería Social?
   - ☑ Si
   - ☐ No

   Si su respuesta es "Si" haga una breve descripción : porque estamos en red, ciencia informacion

9. ¿Conoce usted que es un delito informático?
   - ☑ Si
   - ☐ No

   Si su respuesta es "Si" haga una breve descripción : cuando se aplica, cabe los delitos informa

10. ¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?
    - ☑ Si
    - ☐ No

    Si su respuesta es "Si" mencione la ley : Penal, constitucional

GRACIAS POR SU COLABORACIÓN

3

- **Encuesta 016**

16

Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMA

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e Información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

Edad: [ ] 18 a 24 años [x] 25 a 45 años [ ] 46 años en adelante

Sexo: [ ] Masculino [x] Femenino

1. ¿Cuál es el uso que usted le da al Internet?
   - [x] Para trabajo
   - [ ] Para descargar archivos
   - [x] Para ingresar a redes sociales
   - [ ] Para entretenimiento (descargar/escuchar música, ver videos/películas, jugar, etc).
   - [x] Para realizar compras en línea.
   - [ ] Otros: Para estudio

2. Señale el/los navegadores de Internet que usted utiliza.

   Chrome Mozilla FireFox I Explorer

   - [x] Chrome
   - [x] Firefox
   - [ ] Internet Explorer
   - [ ] Otros:

1

16

Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

3. ¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?
   - [x] Celulares
   - [ ] Tablet
   - [x] Portátiles
   - [x] Computadoras de escritorio
   - [ ] Otros:

4. ¿Usted hace uso de las redes sociales en su lugar de trabajo?
   - [x] Sí
   - [ ] No

   Si su respuesta es "SI" señale que tipo de redes sociales utiliza:
   - [x] Facebook
   - [x] Whatsapp
   - [x] Twiteer
   - [ ] Instagram
   - [x] Correo Electrónico
   - [ ] Otros:

5. ¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).

Mayúsculas	A ...... Z
Minúsculas	a ...... z
Símbolos	/#$%&=¿!¿!|.-_\
Números	0 9

   - [ ] Mayúsculas y minúsculas
   - [ ] Mayúsculas, minúsculas, y símbolos
   - [x] Mayúsculas, minúsculas, símbolos, y números.
   - [ ] Mayúsculas y símbolos.
   - [ ] Mayúsculas y números
   - [ ] Minúsculas y símbolos.
   - [ ] Minúsculas y números
   - [ ] Símbolos y números
   - [ ] Solo mayúsculas
   - [ ] Solo minúsculas
   - [ ] Solo números
   - [ ] Solo símbolos.

6. ¿Para que utiliza usted el correo electrónico asignado por la universidad?
   - [x] Para trabajo
   - [ ] Para descargar archivos personales.
   - [ ] Para el entretenimiento (descargar música, ver películas, jugar, etc)
   - [ ] Para realizar compras en línea.
   - [x] Otro: Actividades en google drive,

2

16

Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

7. ¿Comparte usted información confidencial mediante el uso de las redes sociales?
   - [ ] Sí
   - [x] No

   Si su respuesta es "SI" señale que tipo de información a compartido:
   - [ ] Claves de tarjetas de crédito.
   - [ ] Claves de cuentas electrónicas.
   - [ ] Números de cuentas bancarias
   - [ ] Números de tarjetas de crédito
   - [ ] Número de cedula
   - [ ] Documentos laborales
   - [ ] Otro:

8. ¿Conoce usted acerca de la Ingeniería Social?
   - [x] Sí
   - [ ] No

   Si su respuesta es "SI" haga una breve descripción : Tecnica para obtener informacion confidencial a traves de engaños por parte de los cibercriminales, lo más común y clásico es phishing

9. ¿Conoce usted que es un delito informático?
   - [x] Sí
   - [ ] No

   Si su respuesta es "SI" haga una breve descripción : Actividades ilícitas realizados através de medios y dispositivos tecnológicos, cuyo objetivo es causar daño, provocar perdidas o impedir uso de sistemas informáticos, Actualmente muy conocidos pornografía infantil y fraudes informáticos

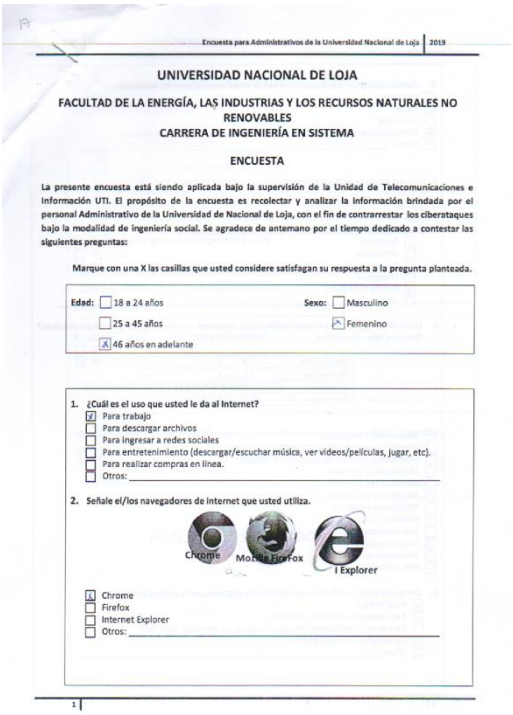
10. ¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?
    - [x] Sí
    - [ ] No

    Si su respuesta es "SI" mencione la ley : Código Orgánico Penal, artículo 178, 230.

GRACIAS POR SU COLABORACIÓN

3

- **Encuesta 017**



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES
CARRERA DE INGENIERÍA EN SISTEMA

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e Información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

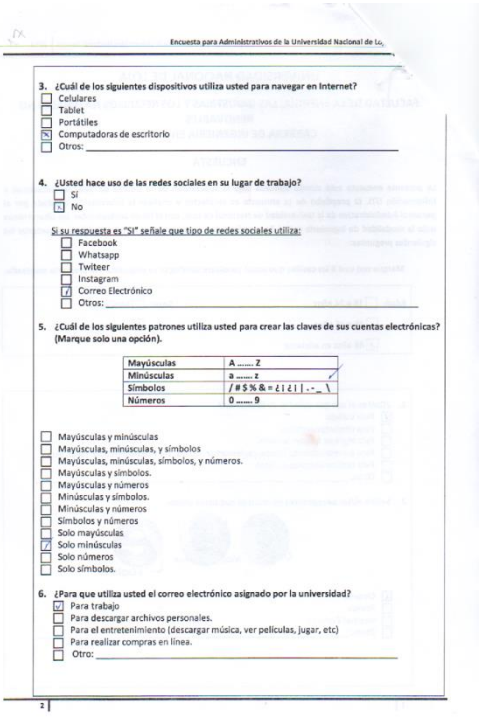
Edad: ☐ 18 a 24 años ☐ 25 a 45 años ☒ 46 años en adelante

Sexo: ☐ Masculino ☒ Femenino

1. **¿Cuál es el uso que usted le da al Internet?**
   - ☒ Para trabajo
   - ☐ Para descargar archivos
   - ☐ Para ingresar a redes sociales
   - ☐ Para entretenimiento (descargar/escuchar música, ver videos/películas, jugar, etc).
   - ☐ Para realizar compras en línea.
   - ☐ Otros: _____
2. **Señale el/los navegadores de internet que usted utiliza.**

   - ☒ Chrome
   - ☐ Firefox
   - ☐ Internet Explorer
   - ☐ Otros: _____

1



Encuesta para Administrativos de la Universidad Nacional de Lo...

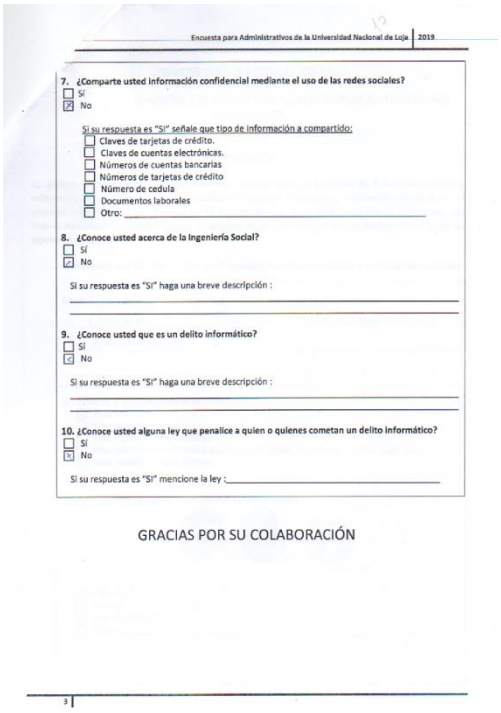
3. **¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?**
   - ☐ Celulares
   - ☐ Tablet
   - ☐ Portátiles
   - ☒ Computadoras de escritorio
   - ☐ Otros: _____
4. **¿Usted hace uso de las redes sociales en su lugar de trabajo?**
   - ☐ Sí
   - ☒ No

   Si su respuesta es "Si" señale que tipo de redes sociales utiliza:
   - ☐ Facebook
   - ☐ Whatsapp
   - ☐ Twiteer
   - ☐ Instagram
   - ☑ Correo Electrónico
   - ☐ Otros: _____
5. **¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).**

Mayúsculas	A ..... Z
Minúsculas	a ..... z
Símbolos	/ # $ % & = ¿ ¡ ¿ ¡ | - - _ \
Números	0 9

   - ☐ Mayúsculas y minúsculas
   - ☐ Mayúsculas, minúsculas, y símbolos
   - ☐ Mayúsculas, minúsculas, símbolos, y números.
   - ☐ Mayúsculas y símbolos.
   - ☐ Mayúsculas y números
   - ☐ Minúsculas y símbolos.
   - ☐ Minúsculas y números
   - ☐ Símbolos y números
   - ☐ Solo mayúsculas
   - ☑ Solo minúsculas
   - ☐ Solo números
   - ☐ Solo símbolos.
6. **¿Para que utiliza usted el correo electrónico asignado por la universidad?**
   - ☑ Para trabajo
   - ☐ Para descargar archivos personales.
   - ☐ Para el entretenimiento (descargar música, ver películas, jugar, etc)
   - ☐ Para realizar compras en línea.
   - ☐ Otro: _____

2



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

7. **¿Comparte usted información confidencial mediante el uso de las redes sociales?**
   - ☐ Sí
   - ☒ No

   Si su respuesta es "Si" señale que tipo de información a compartido:
   - ☐ Claves de tarjetas de crédito.
   - ☐ Claves de cuentas electrónicas.
   - ☐ Números de cuentas bancarias
   - ☐ Números de tarjetas de crédito
   - ☐ Número de cedula
   - ☐ Documentos laborales
   - ☐ Otro: _____
8. **¿Conoce usted acerca de la Ingeniería Social?**
   - ☐ Sí
   - ☑ No

   Si su respuesta es "Si" haga una breve descripción :
   _____
   _____
9. **¿Conoce usted que es un delito informático?**
   - ☐ Sí
   - ☒ No

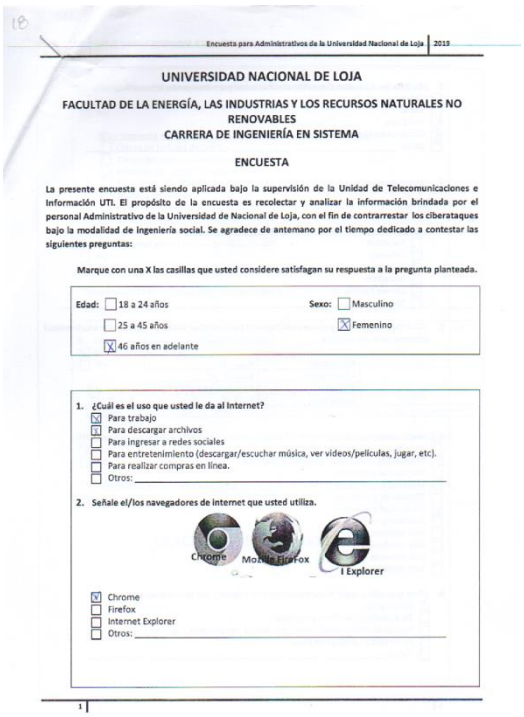
   Si su respuesta es "Si" haga una breve descripción :
   _____
   _____
10. **¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?**
    - ☐ Sí
    - ☒ No

    Si su respuesta es "Si" mencione la ley :_____

GRACIAS POR SU COLABORACIÓN

3

- **Encuesta 018**



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMA

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e Información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de Ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

Edad: ☐ 18 a 24 años ☐ 25 a 45 años ☒ 46 años en adelante

Sexo: ☐ Masculino ☒ Femenino

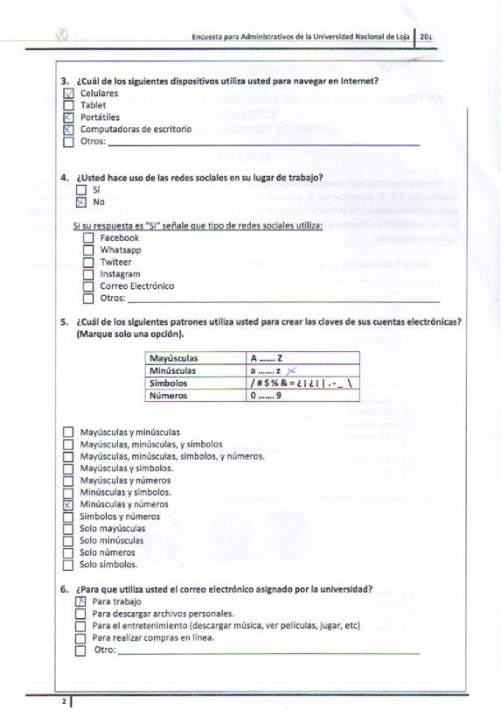
1. ¿Cuál es el uso que usted le da al Internet?
   - ☒ Para trabajo
   - ☒ Para descargar archivos
   - ☐ Para ingresar a redes sociales
   - ☐ Para entretenimiento (descargar/escuchar música, ver videos/películas, jugar, etc).
   - ☐ Para realizar compras en línea.
   - ☐ Otros: _____

2. Señale el/los navegadores de internet que usted utiliza.

   Chrome Mozilla Firefox I Explorer

   - ☒ Chrome
   - ☐ Firefox
   - ☐ Internet Explorer
   - ☐ Otros: _____

1



Encuesta para Administrativos de la Universidad Nacional de Loja | 201

3. ¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?
   - ☒ Celulares
   - ☐ Tablet
   - ☒ Portátiles
   - ☒ Computadoras de escritorio
   - ☐ Otros: _____

4. ¿Usted hace uso de las redes sociales en su lugar de trabajo?
   - ☐ Sí
   - ☒ No

   Si su respuesta es "Sí" señale que tipo de redes sociales utiliza:
   - ☐ Facebook
   - ☐ Whatsapp
   - ☐ Twiteer
   - ☐ Instagram
   - ☐ Correo Electrónico
   - ☐ Otros: _____

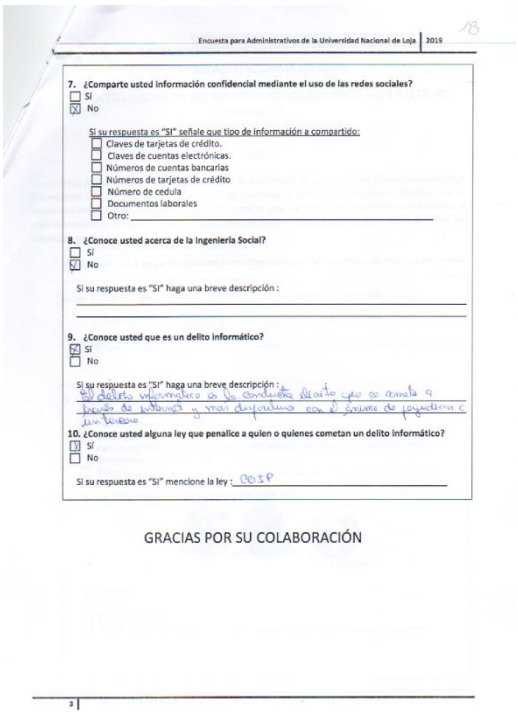
5. ¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).

Mayúsculas	A ..... Z
Minúsculas	a ..... z
Símbolos	/ # $ % & = ¿ ¡ ¿ ¡ | - _ \
Números	0 9

   - ☐ Mayúsculas y minúsculas
   - ☐ Mayúsculas, minúsculas, y símbolos
   - ☐ Mayúsculas, minúsculas, símbolos, y números.
   - ☐ Mayúsculas y símbolos.
   - ☐ Mayúsculas y números
   - ☐ Minúsculas y símbolos.
   - ☒ Minúsculas y números
   - ☐ Símbolos y números
   - ☐ Solo mayúsculas
   - ☐ Solo minúsculas
   - ☐ Solo números
   - ☐ Solo símbolos.

6. ¿Para que utiliza usted el correo electrónico asignado por la universidad?
   - ☒ Para trabajo
   - ☐ Para descargar archivos personales.
   - ☐ Para el entretenimiento (descargar música, ver películas, jugar, etc)
   - ☐ Para realizar compras en línea.
   - ☐ Otro: _____

2



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

7. ¿Comparte usted información confidencial mediante el uso de las redes sociales?
   - ☐ Sí
   - ☒ No

   Si su respuesta es "Sí" señale que tipo de información a compartido:
   - ☐ Claves de tarjetas de crédito.
   - ☐ Claves de cuentas electrónicas.
   - ☐ Números de cuentas bancarias
   - ☐ Números de tarjetas de crédito
   - ☐ Número de cedula
   - ☐ Documentos laborales
   - ☐ Otro: _____

8. ¿Conoce usted acerca de la Ingeniería Social?
   - ☐ Sí
   - ☒ No

   Si su respuesta es "SI" haga una breve descripción : _____

9. ¿Conoce usted que es un delito informático?
   - ☒ Sí
   - ☐ No

   Si su respuesta es "SI" haga una breve descripción : El delito informático es la conducta ilícito que se realiza a través de internet y mas perjudicial para el sistema de seguridad e integridad

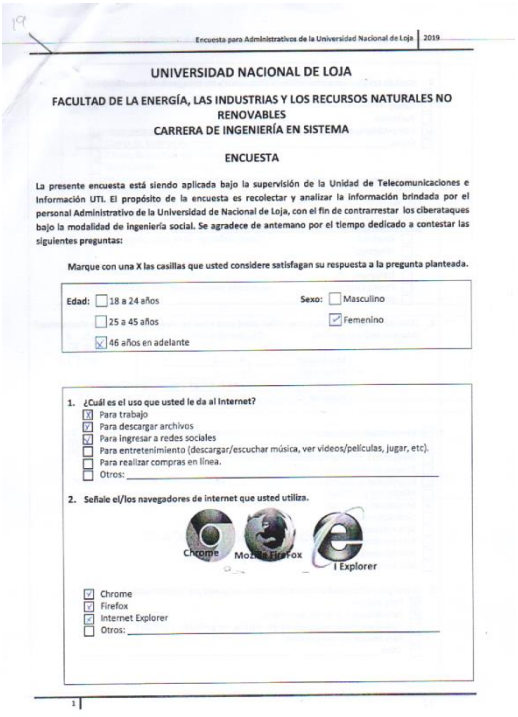
10. ¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?
    - ☒ Sí
    - ☐ No

    Si su respuesta es "SI" mencione la ley : COIP

GRACIAS POR SU COLABORACIÓN

3

- **Encuesta 019**



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMA

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e Información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

Edad: ☐ 18 a 24 años ☐ 25 a 45 años ☒ 46 años en adelante

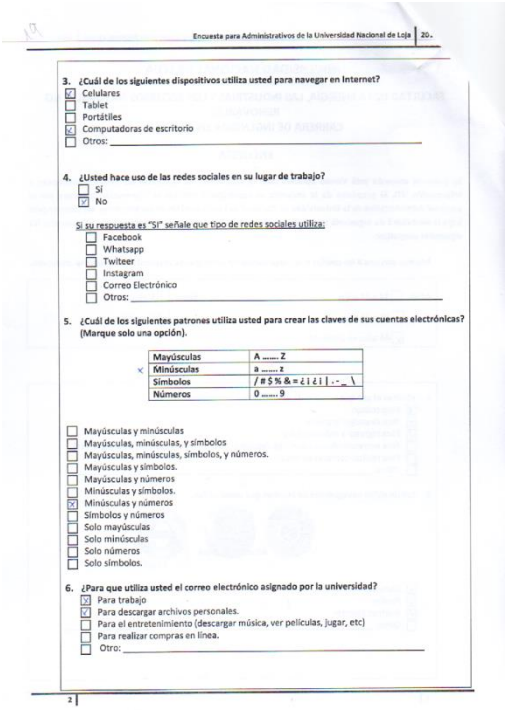
Sexo: ☐ Masculino ☑ Femenino

1. ¿Cuál es el uso que usted le da al Internet?
   - ☒ Para trabajo
   - ☑ Para descargar archivos
   - ☑ Para ingresar a redes sociales
   - ☐ Para entretenimiento (descargar/escuchar música, ver videos/películas, jugar, etc).
   - ☐ Para realizar compras en línea.
   - ☐ Otros: _____

2. Señale el/los navegadores de internet que usted utiliza.

   - ☑ Chrome
   - ☑ Firefox
   - ☑ Internet Explorer
   - ☐ Otros: _____

1



Encuesta para Administrativos de la Universidad Nacional de Loja | 20..

3. ¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?
   - ☑ Celulares
   - ☐ Tablet
   - ☐ Portátiles
   - ☑ Computadoras de escritorio
   - ☐ Otros: _____

4. ¿Usted hace uso de las redes sociales en su lugar de trabajo?
   - ☐ Si
   - ☑ No

   Si su respuesta es "SI" señale que tipo de redes sociales utiliza:
   - ☐ Facebook
   - ☐ Whatsapp
   - ☐ Twiteer
   - ☐ Instagram
   - ☐ Correo Electrónico
   - ☐ Otros: _____

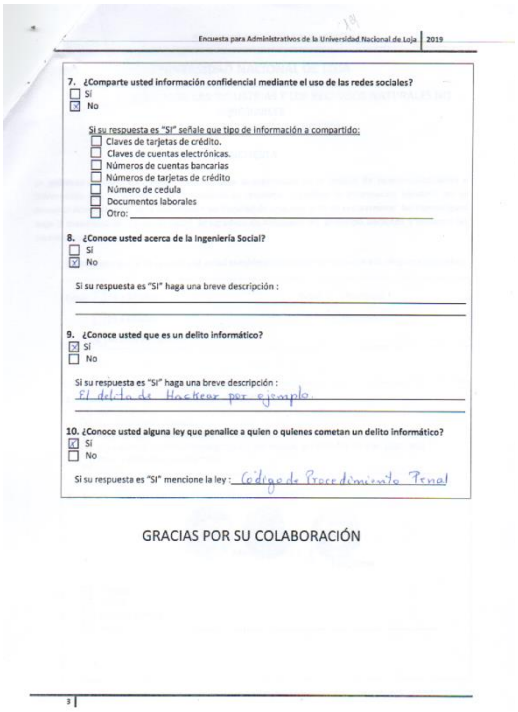
5. ¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).

☒	Mayúsculas	A ..... Z
	Minúsculas	a ..... z
	Símbolos	/ # $ % & = ¿ ¡ ¿ ¡ . - _ \
	Números	0 9

   - ☐ Mayúsculas y minúsculas
   - ☐ Mayúsculas, minúsculas, y símbolos
   - ☐ Mayúsculas, minúsculas, símbolos, y números.
   - ☐ Mayúsculas y símbolos.
   - ☐ Mayúsculas y números
   - ☐ Minúsculas y símbolos.
   - ☒ Minúsculas y números
   - ☐ Símbolos y números
   - ☐ Solo mayúsculas
   - ☐ Solo minúsculas
   - ☐ Solo números
   - ☐ Solo símbolos.

6. ¿Para que utiliza usted el correo electrónico asignado por la universidad?
   - ☑ Para trabajo
   - ☑ Para descargar archivos personales.
   - ☐ Para el entretenimiento (descargar música, ver películas, jugar, etc)
   - ☐ Para realizar compras en línea.
   - ☐ Otro: _____

2



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

7. ¿Comparte usted información confidencial mediante el uso de las redes sociales?
   - ☐ Si
   - ☒ No

   Si su respuesta es "SI" señale que tipo de información a compartido:
   - ☐ Claves de tarjetas de crédito.
   - ☐ Claves de cuentas electrónicas.
   - ☐ Números de cuentas bancarias
   - ☐ Números de tarjetas de crédito
   - ☐ Número de cedula
   - ☐ Documentos laborales
   - ☐ Otro: _____

8. ¿Conoce usted acerca de la Ingeniería Social?
   - ☐ Si
   - ☒ No

   Si su respuesta es "SI" haga una breve descripción :

9. ¿Conoce usted que es un delito informático?
   - ☒ Si
   - ☐ No

   Si su respuesta es "SI" haga una breve descripción :
   El delito de Hackear por ejemplo

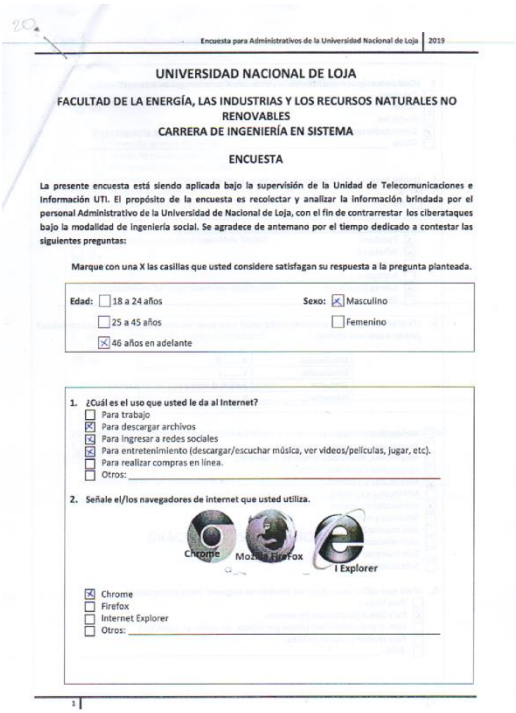
10. ¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?
    - ☒ Si
    - ☐ No

    Si su respuesta es "SI" mencione la ley : Código de Procedimiento Penal

GRACIAS POR SU COLABORACIÓN

3

- **Encuesta 020**



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMA

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e Información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

Edad: ☐ 18 a 24 años ☐ 25 a 45 años ☒ 46 años en adelante

Sexo: ☒ Masculino ☐ Femenino

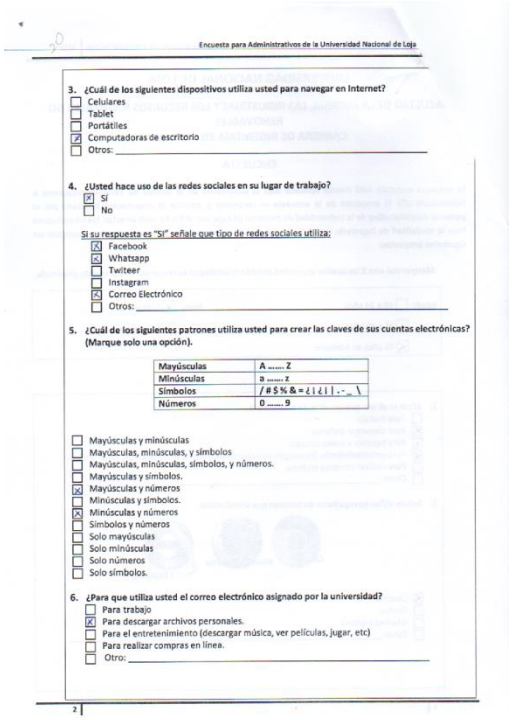
1. ¿Cuál es el uso que usted le da al Internet?
- ☐ Para trabajo
- ☒ Para descargar archivos
- ☒ Para ingresar a redes sociales
- ☒ Para entretenimiento (descargar/escuchar música, ver videos/películas, jugar, etc).
- ☐ Para realizar compras en línea.
- ☐ Otros: _____

2. Señale el/los navegadores de internet que usted utiliza.

Chrome Mozilla FireFox I Explorer

- ☒ Chrome
- ☐ Firefox
- ☐ Internet Explorer
- ☐ Otros: _____

1



Encuesta para Administrativos de la Universidad Nacional de Loja

3. ¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?
- ☐ Celulares
- ☐ Tablet
- ☐ Portátiles
- ☒ Computadoras de escritorio
- ☐ Otros: _____

4. ¿Usted hace uso de las redes sociales en su lugar de trabajo?
- ☒ Si
- ☐ No

Si su respuesta es "Si" señale que tipo de redes sociales utiliza:
- ☒ Facebook
- ☒ Whatsapp
- ☐ Twiteer
- ☐ Instagram
- ☒ Correo Electrónico
- ☐ Otros: _____

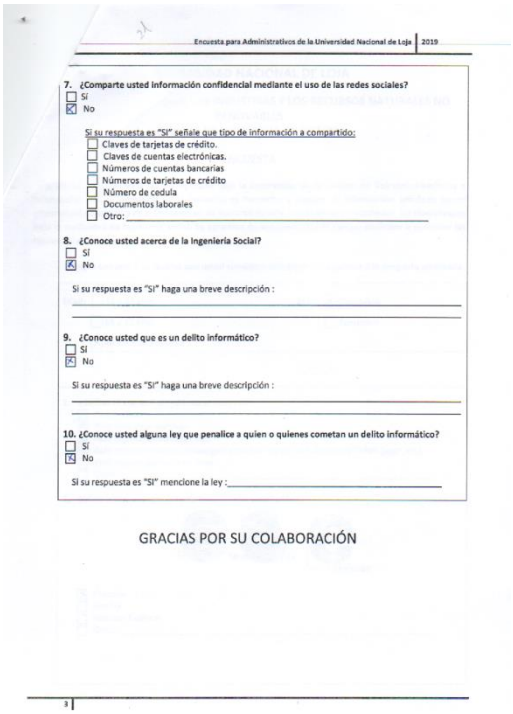
5. ¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).

Mayúsculas	A ..... Z
Minúsculas	a ..... z
Símbolos	/ # $ % & = ¿ ¡ ¿ ¡ ! . - _ \
Números	0 9

- ☐ Mayúsculas y minúsculas
- ☐ Mayúsculas, minúsculas, y símbolos
- ☐ Mayúsculas, minúsculas, símbolos, y números.
- ☐ Mayúsculas y símbolos.
- ☒ Mayúsculas y números
- ☐ Minúsculas y símbolos.
- ☒ Minúsculas y números
- ☐ Símbolos y números
- ☐ Solo mayúsculas
- ☐ Solo minúsculas
- ☐ Solo números
- ☐ Solo símbolos.

6. ¿Para que utiliza usted el correo electrónico asignado por la universidad?
- ☐ Para trabajo
- ☒ Para descargar archivos personales.
- ☐ Para el entretenimiento (descargar música, ver películas, jugar, etc)
- ☐ Para realizar compras en línea.
- ☐ Otro: _____

2



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

7. ¿Comparte usted información confidencial mediante el uso de las redes sociales?
- ☐ Si
- ☒ No

Si su respuesta es "Si" señale que tipo de información a compartido:
- ☐ Claves de tarjetas de crédito.
- ☐ Claves de cuentas electrónicas.
- ☐ Números de cuentas bancarias
- ☐ Números de tarjetas de crédito
- ☐ Número de cedula
- ☐ Documentos laborales
- ☐ Otro: _____

8. ¿Conoce usted acerca de la Ingeniería Social?
- ☐ Si
- ☒ No

Si su respuesta es "Si" haga una breve descripción :

_____

_____

9. ¿Conoce usted que es un delito informático?
- ☐ Si
- ☒ No

Si su respuesta es "Si" haga una breve descripción :

_____

_____

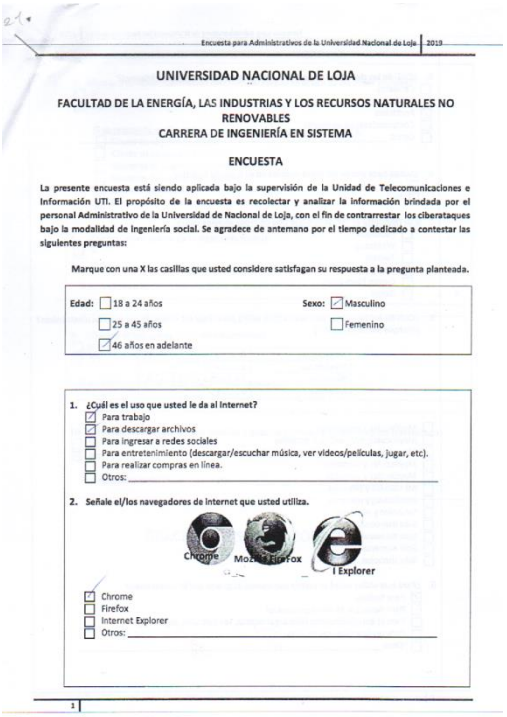
10. ¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?
- ☐ Si
- ☒ No

Si su respuesta es "Si" mencione la ley : _____

GRACIAS POR SU COLABORACIÓN

3

- **Encuesta 021**



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMA

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e Información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

Edad: ☐ 18 a 24 años ☐ 25 a 45 años ☑ 46 años en adelante

Sexo: ☑ Masculino ☐ Femenino

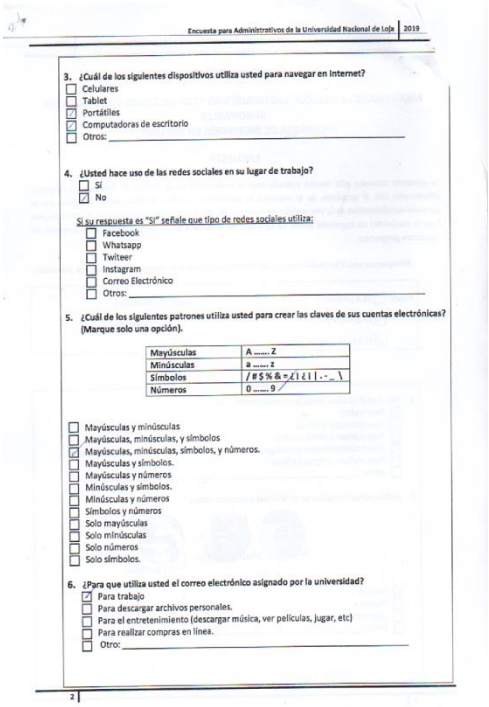
1. ¿Cuál es el uso que usted le da al Internet?
- ☑ Para trabajo
- ☑ Para descargar archivos
- ☐ Para ingresar a redes sociales
- ☐ Para entretenimiento (descargar/escuchar música, ver videos/películas, jugar, etc).
- ☐ Para realizar compras en línea.
- ☐ Otros: _____

2. Señale el/los navegadores de internet que usted utiliza.

Chrome Mozilla Firefox I Explorer

- ☑ Chrome
- ☐ Firefox
- ☐ Internet Explorer
- ☐ Otros: _____

1



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

3. ¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?
- ☐ Celulares
- ☐ Tablet
- ☑ Portátiles
- ☑ Computadoras de escritorio
- ☐ Otros: _____

4. ¿Usted hace uso de las redes sociales en su lugar de trabajo?
- ☐ Si
- ☑ No

Si su respuesta es "Si" señale que tipo de redes sociales utiliza:
- ☐ Facebook
- ☐ Whatsapp
- ☐ Twiteer
- ☐ Instagram
- ☐ Correo Electrónico
- ☐ Otros: _____

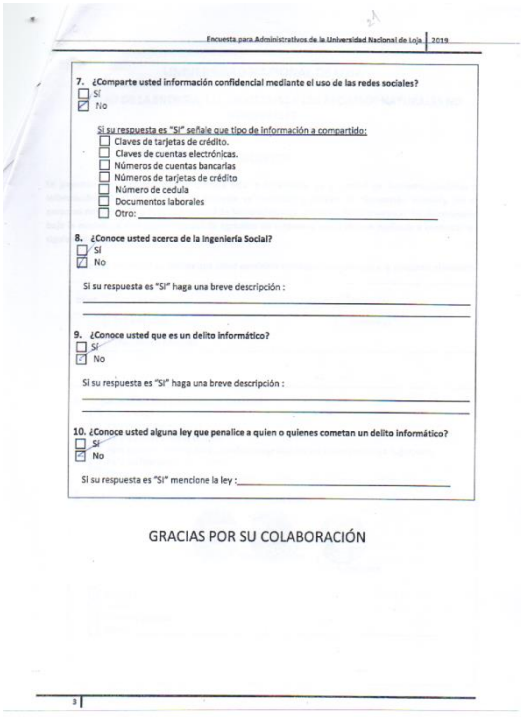
5. ¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).

Mayúsculas	A ..... Z
Minúsculas	a ..... z
Símbolos	/ # $ % & = ¿ ¡ ¡ . - _ \
Números	0 9

- ☐ Mayúsculas y minúsculas
- ☐ Mayúsculas, minúsculas, y símbolos
- ☑ Mayúsculas, minúsculas, símbolos, y números.
- ☐ Mayúsculas y símbolos.
- ☐ Mayúsculas y números
- ☐ Minúsculas y símbolos.
- ☐ Minúsculas y números
- ☐ Símbolos y números
- ☐ Solo mayúsculas
- ☐ Solo minúsculas
- ☐ Solo números
- ☐ Solo símbolos.

6. ¿Para que utiliza usted el correo electrónico asignado por la universidad?
- ☑ Para trabajo
- ☐ Para descargar archivos personales.
- ☐ Para el entretenimiento (descargar música, ver películas, jugar, etc)
- ☐ Para realizar compras en línea.
- ☐ Otro: _____

2



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

7. ¿Comparte usted información confidencial mediante el uso de las redes sociales?
- ☐ Si
- ☑ No

Si su respuesta es "Si" señale que tipo de información a compartido:
- ☐ Claves de tarjetas de crédito.
- ☐ Claves de cuentas electrónicas.
- ☐ Números de cuentas bancarias
- ☐ Números de tarjetas de crédito
- ☐ Número de cedula
- ☐ Documentos laborales
- ☐ Otro: _____

8. ¿Conoce usted acerca de la ingeniería Social?
- ☐ Si
- ☑ No

Si su respuesta es "Si" haga una breve descripción : _____

9. ¿Conoce usted que es un delito informático?
- ☐ Si
- ☑ No

Si su respuesta es "Si" haga una breve descripción : _____

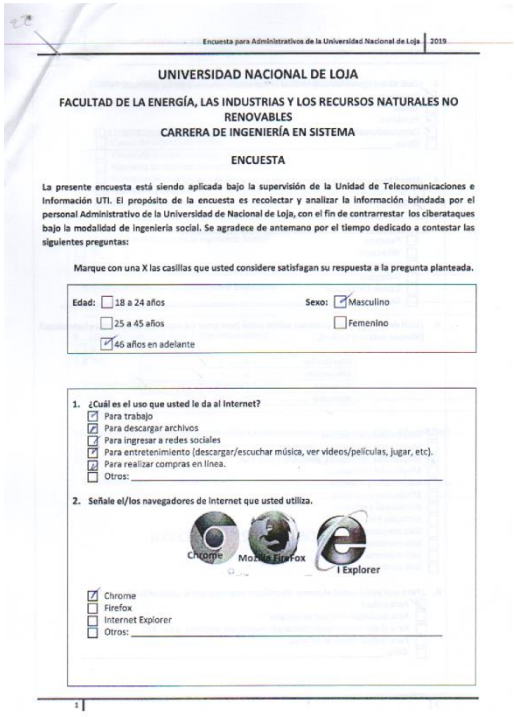
10. ¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?
- ☐ Si
- ☑ No

Si su respuesta es "Si" mencione la ley : _____

GRACIAS POR SU COLABORACIÓN

3

- **Encuesta 022**



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMA

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e Información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

Edad: ☐ 18 a 24 años ☐ 25 a 45 años ☑ 46 años en adelante

Sexo: ☑ Masculino ☐ Femenino

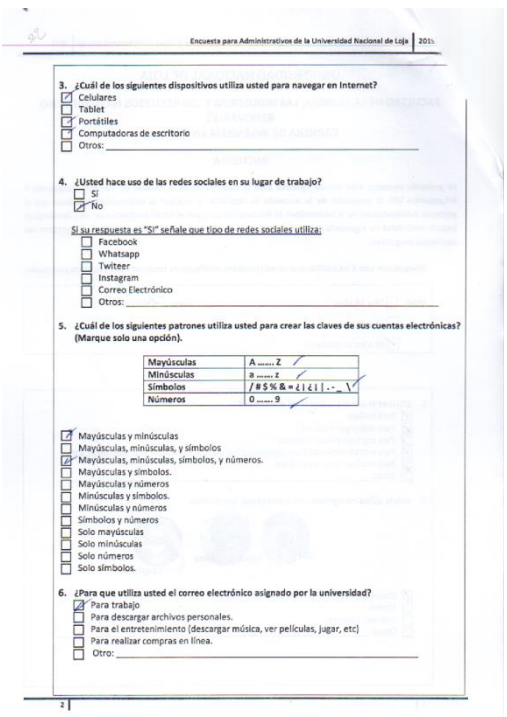
1. ¿Cuál es el uso que usted le da al Internet?
   - ☑ Para trabajo
   - ☑ Para descargar archivos
   - ☑ Para ingresar a redes sociales
   - ☑ Para entretenimiento (descargar/escuchar música, ver videos/películas, jugar, etc).
   - ☑ Para realizar compras en línea.
   - ☐ Otros: _____

2. Señale el/los navegadores de Internet que usted utiliza.

   Chrome Mozilla FireFox I Explorer

   - ☑ Chrome
   - ☐ Firefox
   - ☐ Internet Explorer
   - ☐ Otros: _____

1



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

3. ¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?
   - ☑ Celulares
   - ☐ Tablet
   - ☑ Portátiles
   - ☐ Computadoras de escritorio
   - ☐ Otros: _____

4. ¿Usted hace uso de las redes sociales en su lugar de trabajo?
   - ☐ Si
   - ☑ No

   Si su respuesta es "Si" señale que tipo de redes sociales utiliza:
   - ☐ Facebook
   - ☐ Whatsapp
   - ☐ Twiteer
   - ☐ Instagram
   - ☐ Correo Electrónico
   - ☐ Otros: _____

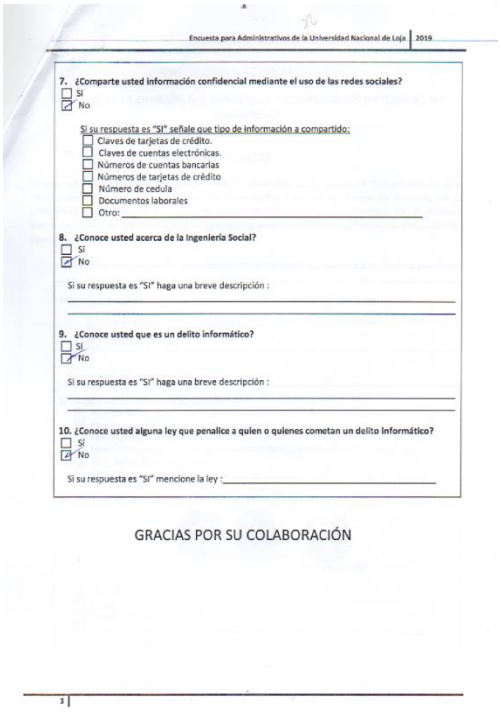
5. ¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).

Mayúsculas	A ..... Z
Minúsculas	a ..... z
Símbolos	/ # $ % & = ¿ ¡ ¡ ¡ . - _
Números	0 9

   - ☑ Mayúsculas y minúsculas
   - ☐ Mayúsculas, minúsculas, y símbolos
   - ☑ Mayúsculas, minúsculas, símbolos, y números.
   - ☐ Mayúsculas y símbolos.
   - ☐ Mayúsculas y números
   - ☐ Minúsculas y símbolos.
   - ☐ Minúsculas y números
   - ☐ Símbolos y números
   - ☐ Solo mayúsculas
   - ☐ Solo minúsculas
   - ☐ Solo números
   - ☐ Solo símbolos.

6. ¿Para que utiliza usted el correo electrónico asignado por la universidad?
   - ☑ Para trabajo
   - ☐ Para descargar archivos personales.
   - ☐ Para el entretenimiento (descargar música, ver películas, jugar, etc)
   - ☐ Para realizar compras en línea.
   - ☐ Otro: _____

2



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

7. ¿Comparte usted información confidencial mediante el uso de las redes sociales?
   - ☐ Si
   - ☑ No

   Si su respuesta es "Si" señale que tipo de información a compartido:
   - ☐ Claves de tarjetas de crédito.
   - ☐ Claves de cuentas electrónicas.
   - ☐ Números de cuentas bancarias
   - ☐ Números de tarjetas de crédito
   - ☐ Número de cedula
   - ☐ Documentos laborales
   - ☐ Otro: _____

8. ¿Conoce usted acerca de la Ingeniería Social?
   - ☐ Si
   - ☑ No

   Si su respuesta es "Si" haga una breve descripción : _____

9. ¿Conoce usted que es un delito informático?
   - ☐ Si
   - ☑ No

   Si su respuesta es "Si" haga una breve descripción : _____

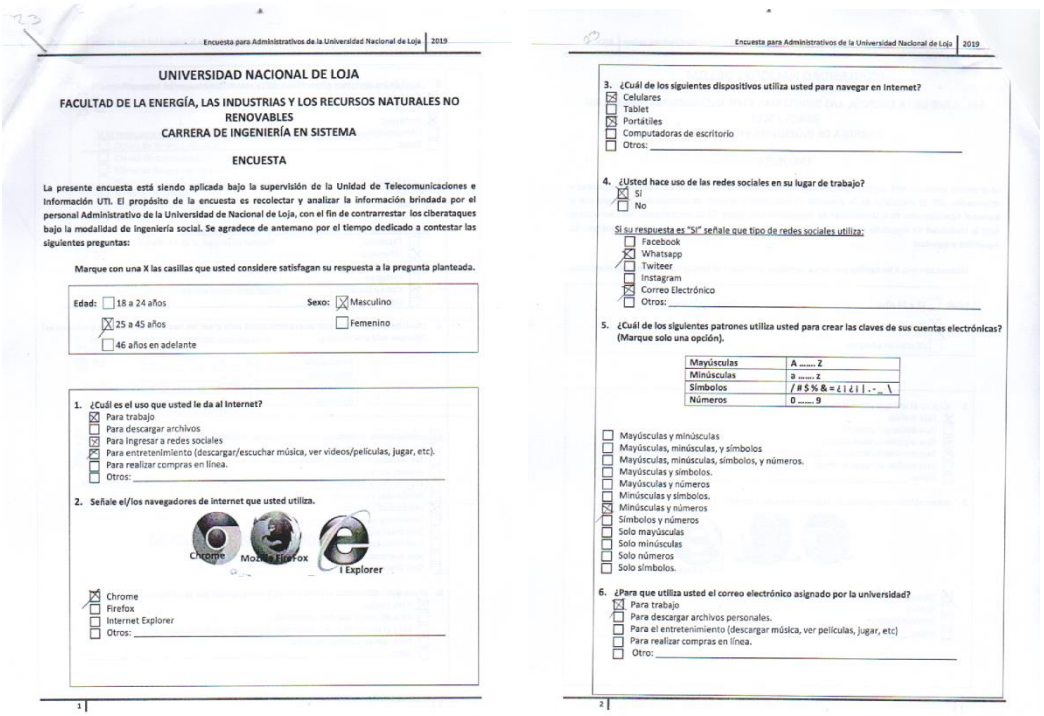
10. ¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?
    - ☐ Si
    - ☑ No

    Si su respuesta es "Si" mencione la ley : _____

GRACIAS POR SU COLABORACIÓN

3

- **Encuesta 023**



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMA

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e Información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

Edad: ☐ 18 a 24 años ☒ 25 a 45 años ☐ 46 años en adelante

Sexo: ☒ Masculino ☐ Femenino

1. ¿Cuál es el uso que usted le da al Internet?
   - ☒ Para trabajo
   - ☐ Para descargar archivos
   - ☒ Para ingresar a redes sociales
   - ☒ Para entretenimiento (descargar/escuchar música, ver videos/películas, jugar, etc).
   - ☐ Para realizar compras en línea.
   - ☐ Otros: _____

2. Señale el/los navegadores de internet que usted utiliza.

   - ☒ Chrome
   - ☐ Firefox
   - ☐ Internet Explorer
   - ☐ Otros: _____

1

Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

3. ¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?
   - ☒ Celulares
   - ☐ Tablet
   - ☒ Portátiles
   - ☐ Computadoras de escritorio
   - ☐ Otros: _____

4. ¿Usted hace uso de las redes sociales en su lugar de trabajo?
   - ☒ Si
   - ☐ No

   Si su respuesta es "Si" señale que tipo de redes sociales utiliza:
   - ☐ Facebook
   - ☒ Whatsapp
   - ☐ Twiteer
   - ☐ Instagram
   - ☒ Correo Electrónico
   - ☐ Otros: _____

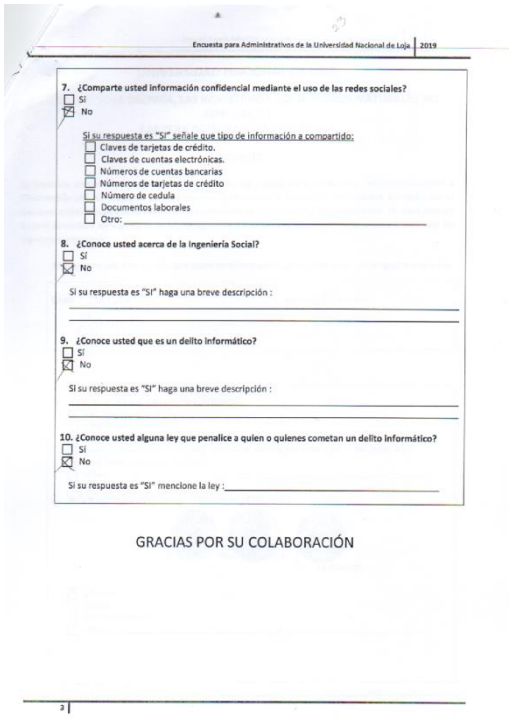
5. ¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).

Mayúsculas	A ..... Z
Minúsculas	a ..... z
Símbolos	/ # $ % & = ¿ ¡ ¿ | . - _ \
Números	0 9

   - ☐ Mayúsculas y minúsculas
   - ☐ Mayúsculas, minúsculas, y símbolos
   - ☐ Mayúsculas, minúsculas, símbolos, y números.
   - ☐ Mayúsculas y símbolos.
   - ☐ Mayúsculas y números
   - ☐ Minúsculas y símbolos.
   - ☒ Minúsculas y números
   - ☐ Símbolos y números
   - ☐ Solo mayúsculas
   - ☐ Solo minúsculas
   - ☐ Solo números
   - ☐ Solo símbolos.

6. ¿Para que utiliza usted el correo electrónico asignado por la universidad?
   - ☒ Para trabajo
   - ☐ Para descargar archivos personales.
   - ☐ Para el entretenimiento (descargar música, ver películas, jugar, etc)
   - ☐ Para realizar compras en línea.
   - ☐ Otro: _____

2



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

7. ¿Comparte usted información confidencial mediante el uso de las redes sociales?
   - ☐ Si
   - ☒ No

   Si su respuesta es "Si" señale que tipo de información a compartido:
   - ☐ Claves de tarjetas de crédito.
   - ☐ Claves de cuentas electrónicas.
   - ☐ Números de cuentas bancarias
   - ☐ Números de tarjetas de crédito
   - ☐ Número de cedula
   - ☐ Documentos laborales
   - ☐ Otro: _____

8. ¿Conoce usted acerca de la Ingeniería Social?
   - ☐ Si
   - ☒ No

   Si su respuesta es "Si" haga una breve descripción :

9. ¿Conoce usted que es un delito informático?
   - ☐ Si
   - ☒ No

   Si su respuesta es "Si" haga una breve descripción :

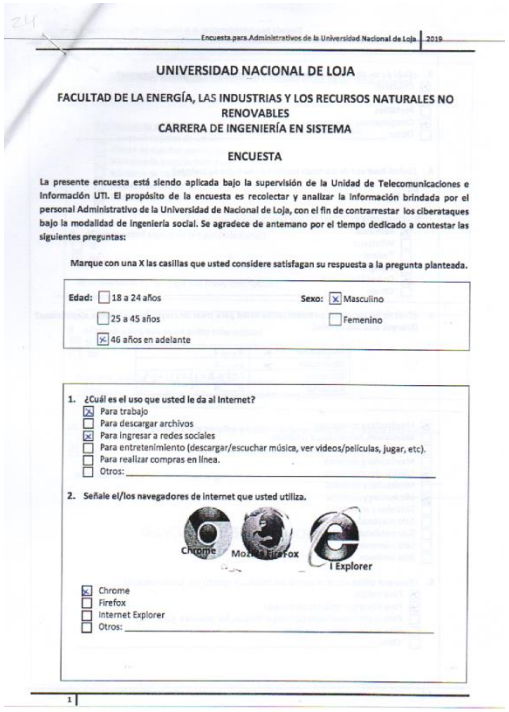
10. ¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?
    - ☐ Si
    - ☒ No

    Si su respuesta es "Si" mencione la ley : _____

GRACIAS POR SU COLABORACIÓN

3

- **Encuesta 024**



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMA

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e Información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

Edad: ☐ 18 a 24 años ☐ 25 a 45 años ☒ 46 años en adelante

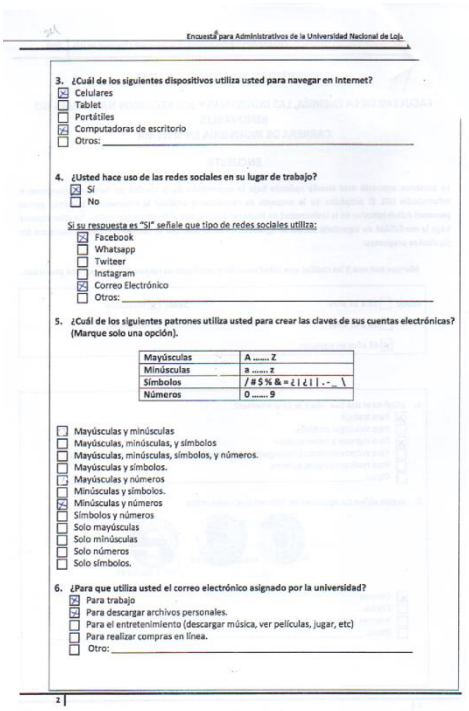
Sexo: ☒ Masculino ☐ Femenino

1. ¿Cuál es el uso que usted le da al Internet?
   - ☒ Para trabajo
   - ☐ Para descargar archivos
   - ☒ Para ingresar a redes sociales
   - ☐ Para entretenimiento (descargar/escuchar música, ver videos/películas, jugar, etc).
   - ☐ Para realizar compras en línea.
   - ☐ Otros: _____

2. Señale el/los navegadores de internet que usted utiliza.

   - ☒ Chrome
   - ☐ Firefox
   - ☐ Internet Explorer
   - ☐ Otros: _____

1



Encuesta para Administrativos de la Universidad Nacional de Loja

3. ¿Cuál de los siguientes dispositivos utiliza usted para navegar en internet?
   - ☒ Celulares
   - ☐ Tablet
   - ☐ Portátiles
   - ☒ Computadoras de escritorio
   - ☐ Otros: _____

4. ¿Usted hace uso de las redes sociales en su lugar de trabajo?
   - ☒ Sí
   - ☐ No

   Si su respuesta es "Si" señale que tipo de redes sociales utiliza:
   - ☒ Facebook
   - ☐ Whatsapp
   - ☐ Twiteer
   - ☐ Instagram
   - ☒ Correo Electrónico
   - ☐ Otros: _____

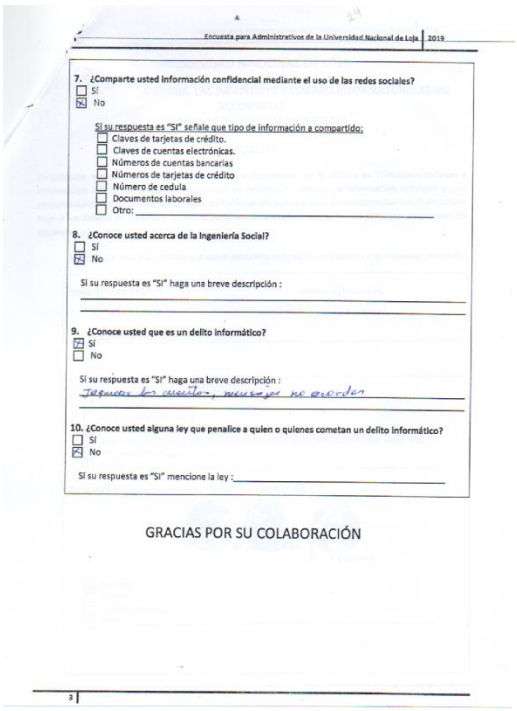
5. ¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).

Mayúsculas	A ..... Z
Minúsculas	a ..... z
Símbolos	/ # $ % & = ¿ ¡ ¡ | . - _ \
Números	0 9

   - ☐ Mayúsculas y minúsculas
   - ☐ Mayúsculas, minúsculas, y símbolos
   - ☐ Mayúsculas, minúsculas, símbolos, y números.
   - ☐ Mayúsculas y símbolos.
   - ☐ Mayúsculas y números
   - ☐ Minúsculas y símbolos.
   - ☒ Minúsculas y números
   - ☐ Símbolos y números
   - ☐ Solo mayúsculas
   - ☐ Solo minúsculas
   - ☐ Solo números
   - ☐ Solo símbolos.

6. ¿Para que utiliza usted el correo electrónico asignado por la universidad?
   - ☒ Para trabajo
   - ☒ Para descargar archivos personales.
   - ☐ Para el entretenimiento (descargar música, ver películas, jugar, etc)
   - ☐ Para realizar compras en línea.
   - ☐ Otro: _____

2



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

7. ¿Comparte usted información confidencial mediante el uso de las redes sociales?
   - ☐ Sí
   - ☒ No

   Si su respuesta es "Si" señale que tipo de información a compartido:
   - ☐ Claves de tarjetas de crédito.
   - ☐ Claves de cuentas electrónicas.
   - ☐ Números de cuentas bancarias
   - ☐ Números de tarjetas de crédito
   - ☐ Número de cedula
   - ☐ Documentos laborales
   - ☐ Otro: _____

8. ¿Conoce usted acerca de la Ingeniería Social?
   - ☐ Sí
   - ☒ No

   Si su respuesta es "Si" haga una breve descripción : _____

9. ¿Conoce usted que es un delito informático?
   - ☒ Sí
   - ☐ No

   Si su respuesta es "Si" haga una breve descripción : Tengan los cuidados, mensajes no abrirlos

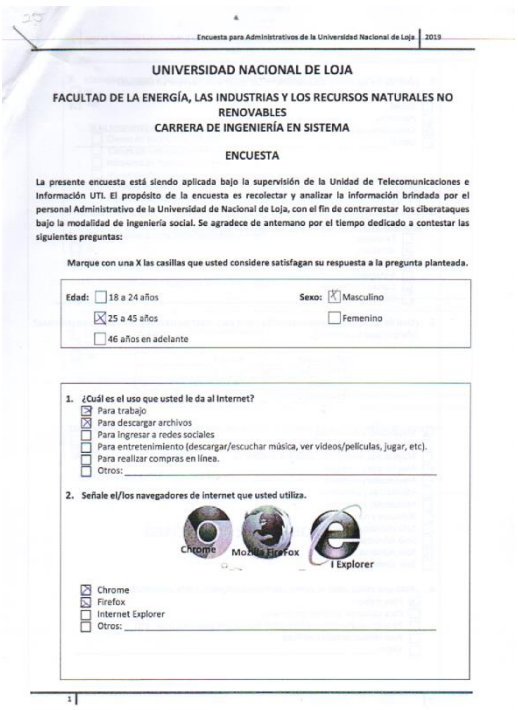
10. ¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?
    - ☐ Sí
    - ☒ No

    Si su respuesta es "Si" mencione la ley : _____

GRACIAS POR SU COLABORACIÓN

3

- **Encuesta 025**



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMA

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e Información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

Edad: ☐ 18 a 24 años ☒ 25 a 45 años ☐ 46 años en adelante

Sexo: ☒ Masculino ☐ Femenino

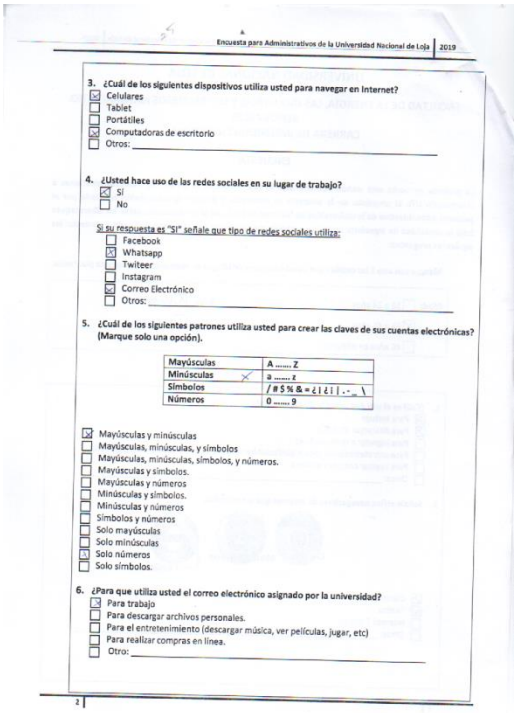
1. ¿Cuál es el uso que usted le da al Internet?
   - ☒ Para trabajo
   - ☒ Para descargar archivos
   - ☐ Para ingresar a redes sociales
   - ☐ Para entretenimiento (descargar/escuchar música, ver videos/películas, jugar, etc).
   - ☐ Para realizar compras en línea.
   - ☐ Otros: _____

2. Señale el/los navegadores de internet que usted utiliza.

   Chrome Mozilla Firefox I Explorer

   - ☒ Chrome
   - ☒ Firefox
   - ☐ Internet Explorer
   - ☐ Otros: _____

1



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

3. ¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?
   - ☒ Celulares
   - ☐ Tablet
   - ☐ Portátiles
   - ☒ Computadoras de escritorio
   - ☐ Otros: _____

4. ¿Usted hace uso de las redes sociales en su lugar de trabajo?
   - ☒ Si
   - ☐ No

   Si su respuesta es "SI" señale que tipo de redes sociales utiliza:
   - ☐ Facebook
   - ☒ Whatsapp
   - ☐ Twiteer
   - ☐ Instagram
   - ☒ Correo Electrónico
   - ☐ Otros: _____

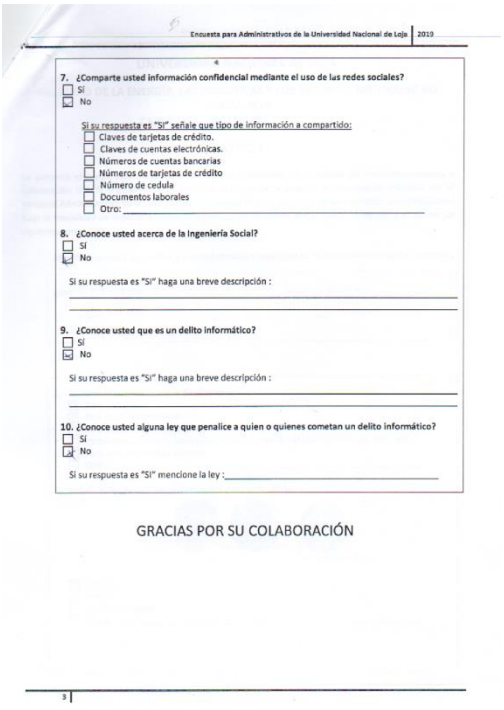
5. ¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).

Mayúsculas	A ..... Z
Minúsculas	a ..... z
Símbolos	/ # $ % & = ¿ ¡ ¿ ¡ | . - _ \
Números	0 9

   - ☒ Mayúsculas y minúsculas
   - ☐ Mayúsculas, minúsculas, y símbolos
   - ☐ Mayúsculas, minúsculas, símbolos, y números.
   - ☐ Mayúsculas y símbolos.
   - ☐ Mayúsculas y números
   - ☐ Minúsculas y símbolos.
   - ☐ Minúsculas y números
   - ☐ Símbolos y números
   - ☐ Solo mayúsculas
   - ☐ Solo minúsculas
   - ☒ Solo números
   - ☐ Solo símbolos.

6. ¿Para que utiliza usted el correo electrónico asignado por la universidad?
   - ☒ Para trabajo
   - ☐ Para descargar archivos personales.
   - ☐ Para el entretenimiento (descargar música, ver películas, jugar, etc)
   - ☐ Para realizar compras en línea.
   - ☐ Otro: _____

2



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

7. ¿Comparte usted información confidencial mediante el uso de las redes sociales?
   - ☐ Si
   - ☒ No

   Si su respuesta es "SI" señale que tipo de información a compartido:
   - ☐ Claves de tarjetas de crédito.
   - ☐ Claves de cuentas electrónicas.
   - ☐ Números de cuentas bancarias
   - ☐ Números de tarjetas de crédito
   - ☐ Número de cedula
   - ☐ Documentos laborales
   - ☐ Otro: _____

8. ¿Conoce usted acerca de la Ingeniería Social?
   - ☐ Si
   - ☒ No

   Si su respuesta es "Si" haga una breve descripción : _____

9. ¿Conoce usted que es un delito informático?
   - ☐ Si
   - ☒ No

   Si su respuesta es "Si" haga una breve descripción : _____

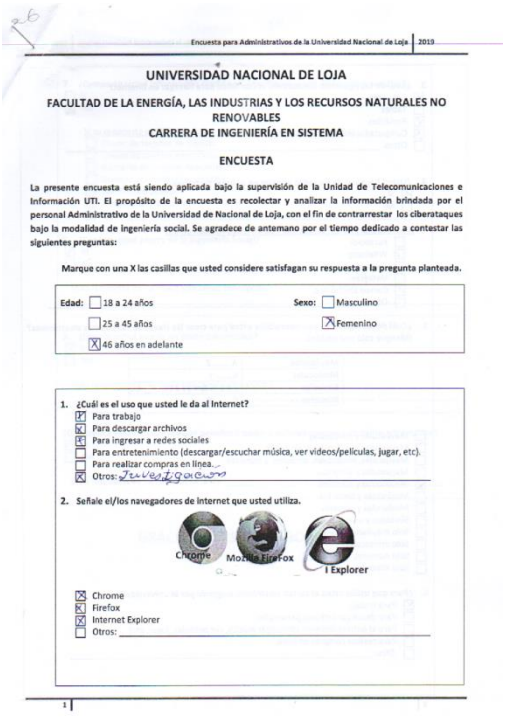
10. ¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?
    - ☐ Si
    - ☒ No

    Si su respuesta es "Si" mencione la ley : _____

GRACIAS POR SU COLABORACIÓN

3

- **Encuesta 026**



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMA

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e Información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

Edad: ☐ 18 a 24 años ☐ 25 a 45 años ☒ 46 años en adelante

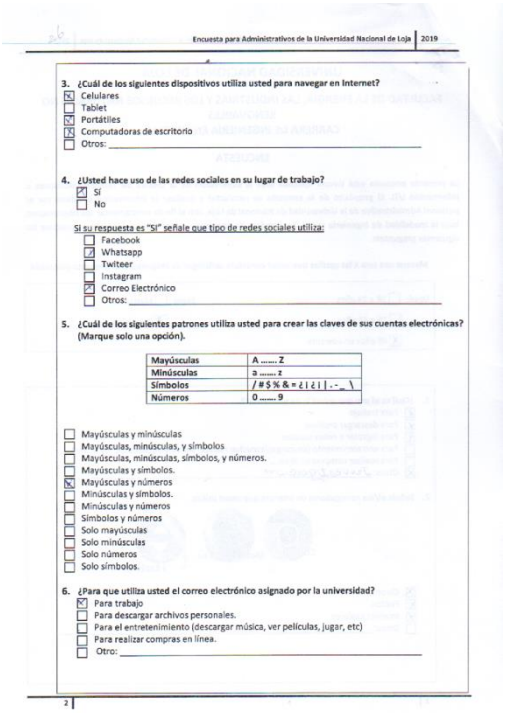
Sexo: ☐ Masculino ☒ Femenino

1. ¿Cuál es el uso que usted le da al Internet?
   - ☒ Para trabajo
   - ☒ Para descargar archivos
   - ☒ Para ingresar a redes sociales
   - ☐ Para entretenimiento (descargar/escuchar música, ver videos/películas, jugar, etc).
   - ☐ Para realizar compras en línea.
   - ☒ Otros: Investigaciones

2. Señale el/los navegadores de internet que usted utiliza.

   - ☒ Chrome
   - ☒ Firefox
   - ☒ Internet Explorer
   - ☐ Otros: _____

1



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

3. ¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?
   - ☒ Celulares
   - ☐ Tablet
   - ☒ Portátiles
   - ☒ Computadoras de escritorio
   - ☐ Otros: _____

4. ¿Usted hace uso de las redes sociales en su lugar de trabajo?
   - ☒ Sí
   - ☐ No

   Si su respuesta es "Sí" señale que tipo de redes sociales utiliza:
   - ☐ Facebook
   - ☒ Whatsapp
   - ☐ Twiteer
   - ☐ Instagram
   - ☒ Correo Electrónico
   - ☐ Otros: _____

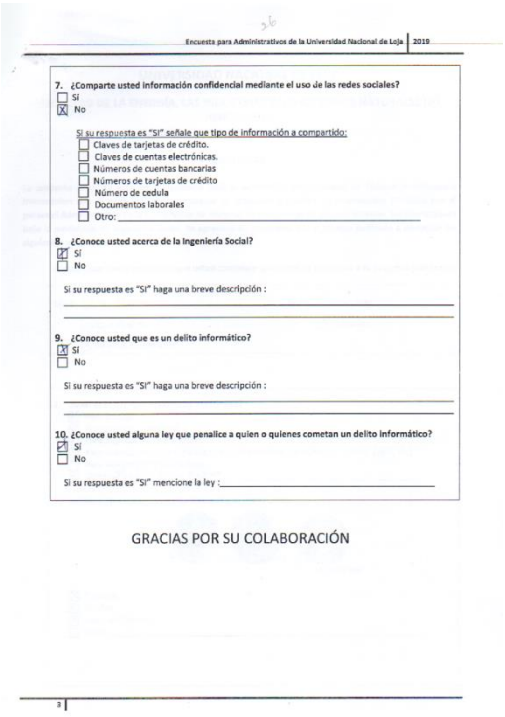
5. ¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).

Mayúsculas	A ..... Z
Minúsculas	a ..... z
Símbolos	/ # $ % & = ¿ ¡ ¦ . - _ \
Números	0 9

   - ☐ Mayúsculas y minúsculas
   - ☐ Mayúsculas, minúsculas, y símbolos
   - ☐ Mayúsculas, minúsculas, símbolos, y números.
   - ☐ Mayúsculas y símbolos.
   - ☒ Mayúsculas y números
   - ☐ Minúsculas y símbolos.
   - ☐ Minúsculas y números
   - ☐ Símbolos y números
   - ☐ Solo mayúsculas
   - ☐ Solo minúsculas
   - ☐ Solo números
   - ☐ Solo símbolos.

6. ¿Para que utiliza usted el correo electrónico asignado por la universidad?
   - ☒ Para trabajo
   - ☐ Para descargar archivos personales.
   - ☐ Para el entretenimiento (descargar música, ver películas, jugar, etc)
   - ☐ Para realizar compras en línea.
   - ☐ Otro: _____

2



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

7. ¿Comparte usted información confidencial mediante el uso de las redes sociales?
   - ☐ Sí
   - ☒ No

   Si su respuesta es "Sí" señale que tipo de información a compartido:
   - ☐ Claves de tarjetas de crédito.
   - ☐ Claves de cuentas electrónicas.
   - ☐ Números de cuentas bancarias
   - ☐ Números de tarjetas de crédito
   - ☐ Número de cedula
   - ☐ Documentos laborales
   - ☐ Otro: _____

8. ¿Conoce usted acerca de la Ingeniería Social?
   - ☒ Sí
   - ☐ No

   Si su respuesta es "Sí" haga una breve descripción : _____

9. ¿Conoce usted que es un delito informático?
   - ☒ Sí
   - ☐ No

   Si su respuesta es "Sí" haga una breve descripción : _____

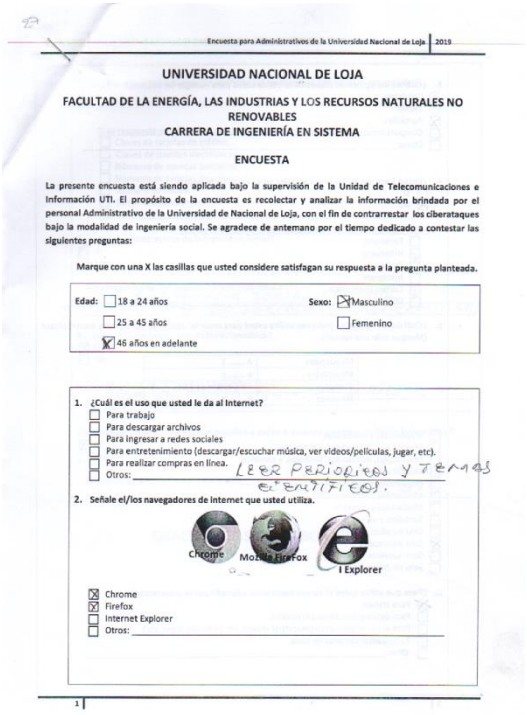
10. ¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?
    - ☒ Sí
    - ☐ No

    Si su respuesta es "Sí" mencione la ley : _____

GRACIAS POR SU COLABORACIÓN

3

- **Encuesta 027**



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES
CARRERA DE INGENIERÍA EN SISTEMA

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e Información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

Edad: ☐ 18 a 24 años ☐ 25 a 45 años ☒ 46 años en adelante

Sexo: ☒ Masculino ☐ Femenino

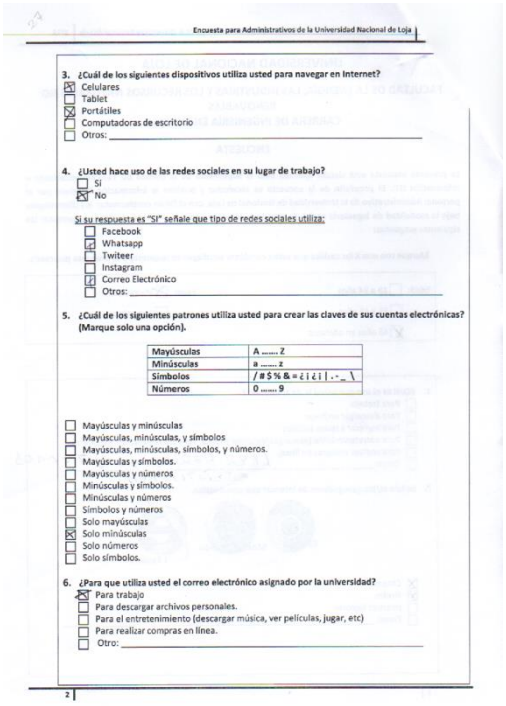
1. ¿Cuál es el uso que usted le da al Internet?
   - ☐ Para trabajo
   - ☐ Para descargar archivos
   - ☐ Para ingresar a redes sociales
   - ☐ Para entretenimiento (descargar/escuchar música, ver videos/películas, jugar, etc).
   - ☐ Para realizar compras en línea.
   - ☐ Otros: LEER PERIODICOS Y TEMAS CIENTIFICOS.

2. Señale el/los navegadores de Internet que usted utiliza.

Chrome Mozilla Firefox I Explorer

- ☒ Chrome
- ☒ Firefox
- ☐ Internet Explorer
- ☐ Otros:

1



Encuesta para Administrativos de la Universidad Nacional de Loja

3. ¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?
   - ☒ Celulares
   - ☐ Tablet
   - ☒ Portátiles
   - ☐ Computadoras de escritorio
   - ☐ Otros:

4. ¿Usted hace uso de las redes sociales en su lugar de trabajo?
   - ☐ Si
   - ☒ No

Si su respuesta es "SI" señale que tipo de redes sociales utiliza:
- ☐ Facebook
- ☑ Whatsapp
- ☐ Twiteer
- ☐ Instagram
- ☑ Correo Electrónico
- ☐ Otros:

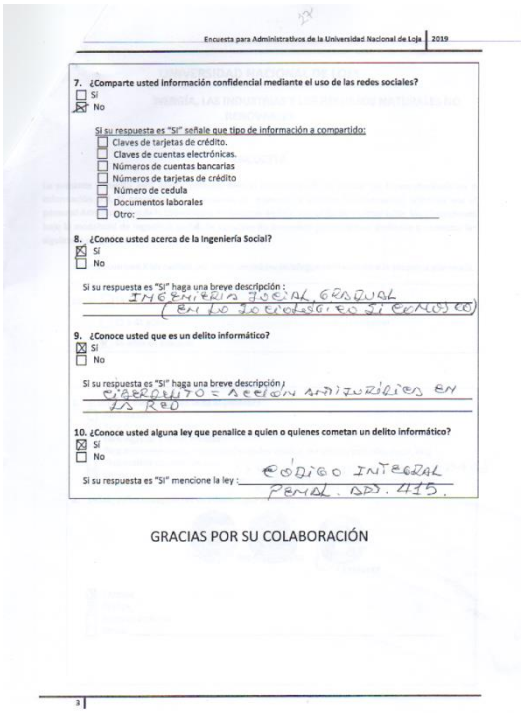
5. ¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).

Mayúsculas	A ..... Z
Minúsculas	a ..... z
Símbolos	/ # $ % & = ¿ ¡ ¿ | . - _ \
Números	0 9

- ☐ Mayúsculas y minúsculas
- ☐ Mayúsculas, minúsculas, y símbolos
- ☐ Mayúsculas, minúsculas, símbolos, y números.
- ☐ Mayúsculas y símbolos.
- ☐ Mayúsculas y números
- ☐ Minúsculas y símbolos.
- ☐ Minúsculas y números
- ☐ Símbolos y números
- ☐ Solo mayúsculas
- ☒ Solo minúsculas
- ☐ Solo números
- ☐ Solo símbolos.

6. ¿Para que utiliza usted el correo electrónico asignado por la universidad?
   - ☒ Para trabajo
   - ☐ Para descargar archivos personales.
   - ☐ Para el entretenimiento (descargar música, ver películas, jugar, etc)
   - ☐ Para realizar compras en línea.
   - ☐ Otro:

2



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

7. ¿Comparte usted información confidencial mediante el uso de las redes sociales?
   - ☐ Si
   - ☒ No

Si su respuesta es "SI" señale que tipo de información a compartido:
- ☐ Claves de tarjetas de crédito.
- ☐ Claves de cuentas electrónicas.
- ☐ Números de cuentas bancarias
- ☐ Números de tarjetas de crédito
- ☐ Número de cedula
- ☐ Documentos laborales
- ☐ Otro:

8. ¿Conoce usted acerca de la Ingeniería Social?
   - ☒ Si
   - ☐ No

Si su respuesta es "SI" haga una breve descripción: INGENIERIA SOCIAL ES UNA (EL ARTE DE ENGAÑAR A LAS PERSONAS)

9. ¿Conoce usted que es un delito informático?
   - ☒ Si
   - ☐ No

Si su respuesta es "SI" haga una breve descripción) DELITO = ACCION ANTIJURIDICA EN LA RED

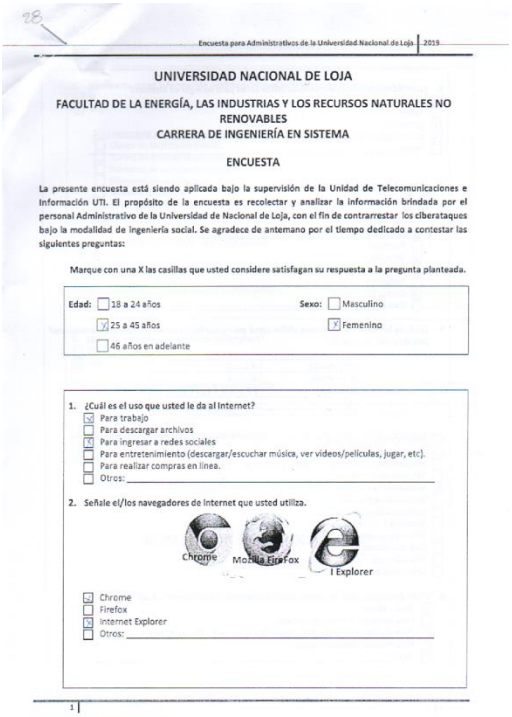
10. ¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?
    - ☒ Si
    - ☐ No

Si su respuesta es "SI" mencione la ley: CODIGO INTEGRAL PENAL. ART. 415.

GRACIAS POR SU COLABORACIÓN

3

- **Encuesta 028**



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMA

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

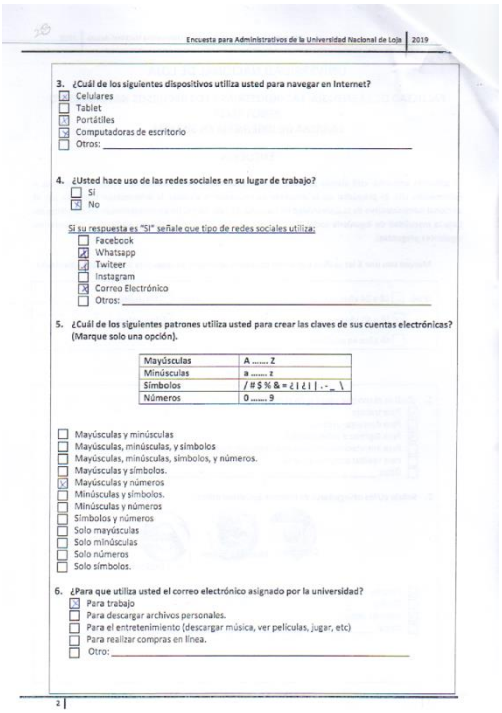
Edad: ☐ 18 a 24 años ☒ 25 a 45 años ☐ 46 años en adelante

Sexo: ☐ Masculino ☒ Femenino

1. ¿Cuál es el uso que usted le da al Internet?
   - ☒ Para trabajo
   - ☐ Para descargar archivos
   - ☒ Para ingresar a redes sociales
   - ☐ Para entretenimiento (descargar/escuchar música, ver videos/películas, jugar, etc).
   - ☐ Para realizar compras en línea.
   - ☐ Otros: _____
2. Señale el/los navegadores de Internet que usted utiliza.

   - ☒ Chrome
   - ☐ Firefox
   - ☐ Internet Explorer
   - ☐ Otros: _____

1



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

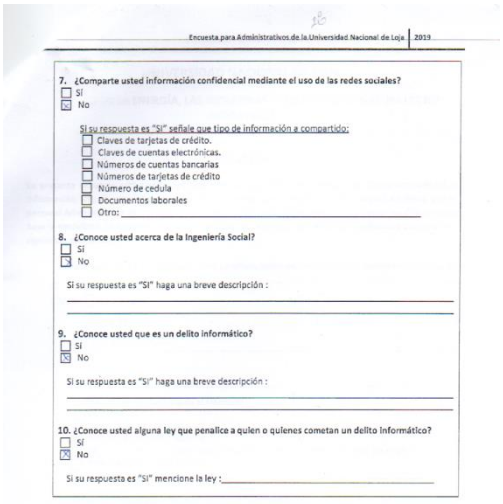
3. ¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?
   - ☒ Celulares
   - ☐ Tablet
   - ☒ Portátiles
   - ☒ Computadoras de escritorio
   - ☐ Otros: _____
4. ¿Usted hace uso de las redes sociales en su lugar de trabajo?
   - ☐ Si
   - ☒ No

   Si su respuesta es "SI" señale que tipo de redes sociales utiliza:
   - ☐ Facebook
   - ☒ Whatsapp
   - ☐ Twiteer
   - ☐ Instagram
   - ☒ Correo Electrónico
   - ☐ Otros: _____
5. ¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).

Mayúsculas	A ..... Z
Minúsculas	a ..... z
Símbolos	/ # $ % & = ¿ ! ¿ ! | . - _ \
Números	0 9

   - ☐ Mayúsculas y minúsculas
   - ☐ Mayúsculas, minúsculas, y símbolos
   - ☐ Mayúsculas, minúsculas, símbolos, y números.
   - ☐ Mayúsculas y símbolos.
   - ☒ Mayúsculas y números
   - ☐ Minúsculas y símbolos.
   - ☐ Minúsculas y números
   - ☐ Símbolos y números
   - ☐ Solo mayúsculas
   - ☐ Solo minúsculas
   - ☐ Solo números
   - ☐ Solo símbolos.
6. ¿Para que utiliza usted el correo electrónico asignado por la universidad?
   - ☒ Para trabajo
   - ☐ Para descargar archivos personales.
   - ☐ Para el entretenimiento (descargar música, ver películas, jugar, etc)
   - ☐ Para realizar compras en línea.
   - ☐ Otro: _____

2



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

7. ¿Comparte usted información confidencial mediante el uso de las redes sociales?
   - ☐ SI
   - ☒ No

   Si su respuesta es "SI" señale que tipo de información a compartido:
   - ☐ Claves de tarjetas de crédito.
   - ☐ Claves de cuentas electrónicas.
   - ☐ Números de cuentas bancarias
   - ☐ Números de tarjetas de crédito
   - ☐ Número de cedula
   - ☐ Documentos laborales
   - ☐ Otro: _____
8. ¿Conoce usted acerca de la Ingeniería Social?
   - ☐ SI
   - ☒ No

   Si su respuesta es "SI" haga una breve descripción : _____
9. ¿Conoce usted que es un delito informático?
   - ☐ SI
   - ☒ No

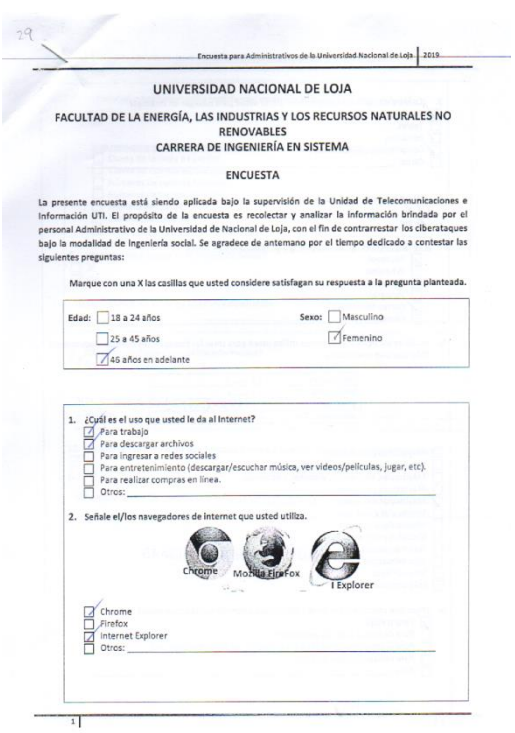
   Si su respuesta es "SI" haga una breve descripción : _____
10. ¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?
    - ☐ SI
    - ☒ No

    Si su respuesta es "SI" mencione la ley : _____

GRACIAS POR SU COLABORACIÓN

3

- **Encuesta 029**



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMA

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e Información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de Ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

Edad: ☐ 18 a 24 años ☐ 25 a 45 años ☑ 46 años en adelante

Sexo: ☐ Masculino ☑ Femenino

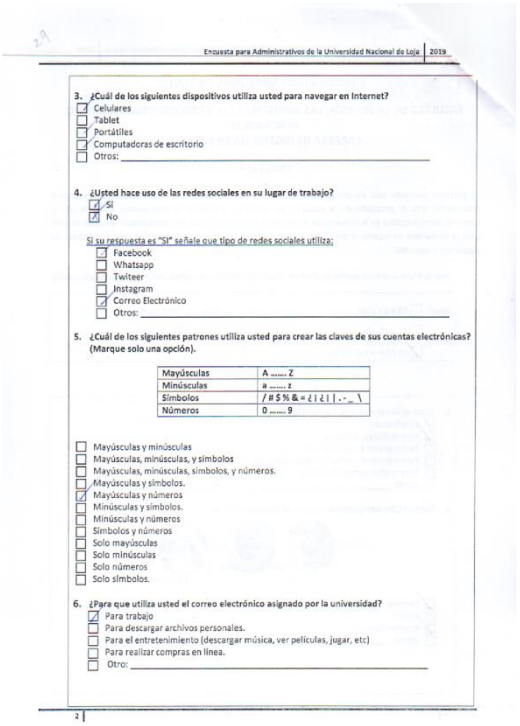
1. ¿Cuál es el uso que usted le da al Internet?
   - ☑ Para trabajo
   - ☑ Para descargar archivos
   - ☐ Para ingresar a redes sociales
   - ☐ Para entretenimiento (descargar/escuchar música, ver videos/películas, jugar, etc).
   - ☐ Para realizar compras en línea.
   - ☐ Otros: _____

2. Señale el/los navegadores de internet que usted utiliza.

   Chrome Mozilla FireFox I Explorer

   - ☑ Chrome
   - ☐ Firefox
   - ☑ Internet Explorer
   - ☐ Otros: _____

1



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

3. ¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?
   - ☑ Celulares
   - ☐ Tablet
   - ☐ Portátiles
   - ☑ Computadoras de escritorio
   - ☐ Otros: _____

4. ¿Usted hace uso de las redes sociales en su lugar de trabajo?
   - ☑ Sí
   - ☑ No

   Si su respuesta es "Sí" señale que tipo de redes sociales utiliza:
   - ☑ Facebook
   - ☐ Whatsapp
   - ☐ Twiteer
   - ☐ Instagram
   - ☑ Correo Electrónico
   - ☐ Otros: _____

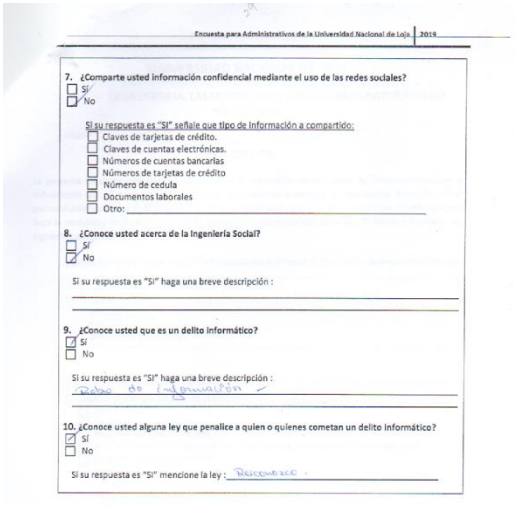
5. ¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).

Mayúsculas	A ..... Z
Minúsculas	a ..... z
Símbolos	/ # $ % & = ¿ ! ¿ ! | . - _ \
Números	0 9

   - ☐ Mayúsculas y minúsculas
   - ☐ Mayúsculas, minúsculas, y símbolos
   - ☐ Mayúsculas, minúsculas, símbolos, y números.
   - ☑ Mayúsculas y símbolos.
   - ☑ Mayúsculas y números
   - ☐ Minúsculas y símbolos.
   - ☐ Minúsculas y números
   - ☐ Símbolos y números
   - ☐ Solo mayúsculas
   - ☐ Solo minúsculas
   - ☐ Solo números
   - ☐ Solo símbolos.

6. ¿Para que utiliza usted el correo electrónico asignado por la universidad?
   - ☑ Para trabajo
   - ☐ Para descargar archivos personales.
   - ☐ Para el entretenimiento (descargar música, ver películas, jugar, etc)
   - ☐ Para realizar compras en línea.
   - ☐ Otro: _____

2



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

7. ¿Comparte usted información confidencial mediante el uso de las redes sociales?
   - ☐ Sí
   - ☑ No

   Si su respuesta es "Sí" señale que tipo de información a compartido:
   - ☐ Claves de tarjetas de crédito.
   - ☐ Claves de cuentas electrónicas.
   - ☐ Números de cuentas bancarias
   - ☐ Números de tarjetas de crédito
   - ☐ Número de cedula
   - ☐ Documentos laborales
   - ☐ Otro: _____

8. ¿Conoce usted acerca de la Ingeniería Social?
   - ☐ Sí
   - ☑ No

   Si su respuesta es "Sí" haga una breve descripción : _____

9. ¿Conoce usted que es un delito informático?
   - ☑ Sí
   - ☐ No

   Si su respuesta es "Sí" haga una breve descripción : _____

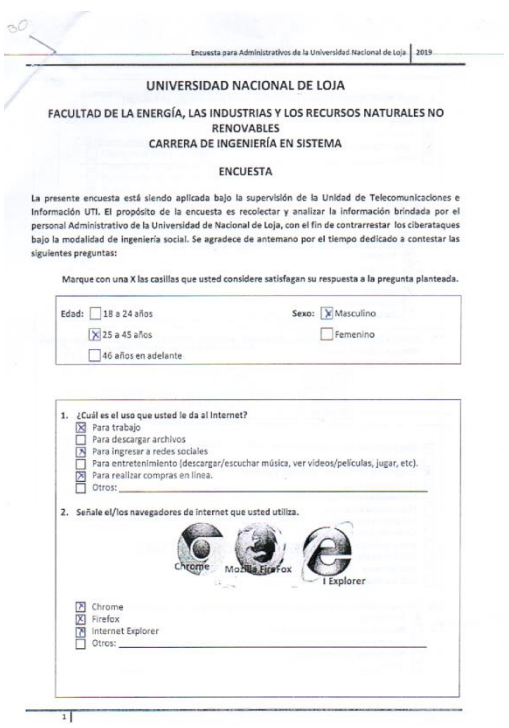
10. ¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?
    - ☑ Sí
    - ☐ No

    Si su respuesta es "Sí" mencione la ley : _____

GRACIAS POR SU COLABORACIÓN

3

- **Encuesta 030**



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

UNIVERSIDAD NACIONAL DE LOJA

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

CARRERA DE INGENIERÍA EN SISTEMA

ENCUESTA

La presente encuesta está siendo aplicada bajo la supervisión de la Unidad de Telecomunicaciones e Información UTI. El propósito de la encuesta es recolectar y analizar la información brindada por el personal Administrativo de la Universidad de Nacional de Loja, con el fin de contrarrestar los ciberataques bajo la modalidad de ingeniería social. Se agradece de antemano por el tiempo dedicado a contestar las siguientes preguntas:

Marque con una X las casillas que usted considere satisfagan su respuesta a la pregunta planteada.

Edad: ☐ 18 a 24 años ☒ 25 a 45 años ☐ 46 años en adelante

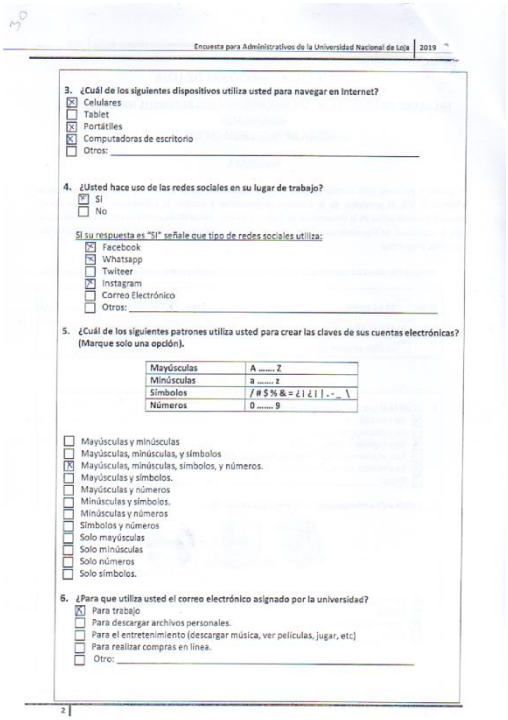
Sexo: ☒ Masculino ☐ Femenino

1. ¿Cuál es el uso que usted le da al Internet?
   - ☒ Para trabajo
   - ☐ Para descargar archivos
   - ☒ Para ingresar a redes sociales
   - ☐ Para entretenimiento (descargar/escuchar música, ver videos/películas, jugar, etc).
   - ☒ Para realizar compras en línea.
   - ☐ Otros: _____

2. Señale el/los navegadores de internet que usted utiliza.

   - ☒ Chrome
   - ☒ Firefox
   - ☒ Internet Explorer
   - ☐ Otros: _____

1



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

3. ¿Cuál de los siguientes dispositivos utiliza usted para navegar en Internet?
   - ☒ Celulares
   - ☐ Tablet
   - ☒ Portátiles
   - ☒ Computadoras de escritorio
   - ☐ Otros: _____

4. ¿Usted hace uso de las redes sociales en su lugar de trabajo?
   - ☒ Si
   - ☐ No

   Si su respuesta es "Si" señale que tipo de redes sociales utiliza:
   - ☒ Facebook
   - ☒ Whatsapp
   - ☐ Twiteer
   - ☒ Instagram
   - ☐ Correo Electrónico
   - ☐ Otros: _____

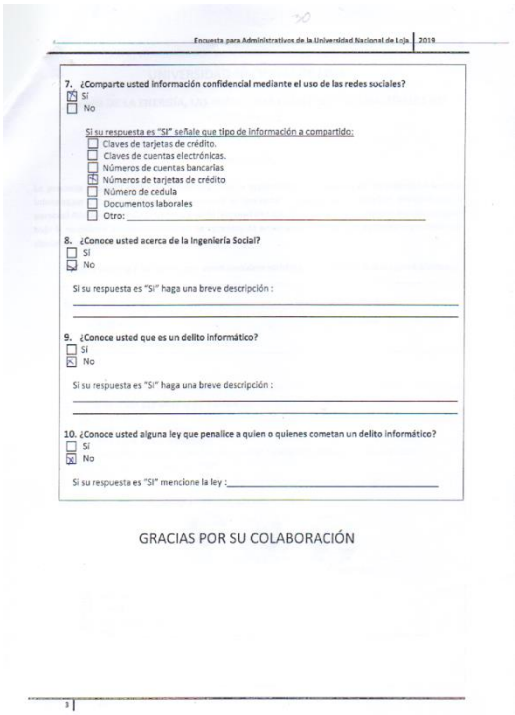
5. ¿Cuál de los siguientes patrones utiliza usted para crear las claves de sus cuentas electrónicas? (Marque solo una opción).

Mayúsculas	A ..... Z
Minúsculas	a ..... z
Símbolos	/ # $ % & = ¿ ! ¿ ! | . - _ \
Números	0 9

   - ☐ Mayúsculas y minúsculas
   - ☐ Mayúsculas, minúsculas, y símbolos
   - ☒ Mayúsculas, minúsculas, símbolos, y números.
   - ☐ Mayúsculas y símbolos.
   - ☐ Mayúsculas y números
   - ☐ Minúsculas y símbolos.
   - ☐ Minúsculas y números
   - ☐ Símbolos y números
   - ☐ Solo mayúsculas
   - ☐ Solo minúsculas
   - ☐ Solo números
   - ☐ Solo símbolos.

6. ¿Para que utiliza usted el correo electrónico asignado por la universidad?
   - ☒ Para trabajo
   - ☐ Para descargar archivos personales.
   - ☐ Para el entretenimiento (descargar música, ver películas, jugar, etc)
   - ☐ Para realizar compras en línea.
   - ☐ Otro: _____

2



Encuesta para Administrativos de la Universidad Nacional de Loja | 2019

7. ¿Comparte usted información confidencial mediante el uso de las redes sociales?
   - ☒ Si
   - ☐ No

   Si su respuesta es "Si" señale que tipo de información a compartido:
   - ☐ Claves de tarjetas de crédito.
   - ☐ Claves de cuentas electrónicas.
   - ☐ Números de cuentas bancarias
   - ☒ Números de tarjetas de crédito
   - ☐ Número de cedula
   - ☐ Documentos laborales
   - ☐ Otro: _____

8. ¿Conoce usted acerca de la Ingeniería Social?
   - ☐ Si
   - ☒ No

   Si su respuesta es "Si" haga una breve descripción : _____

9. ¿Conoce usted que es un delito informático?
   - ☐ Si
   - ☒ No

   Si su respuesta es "Si" haga una breve descripción : _____

10. ¿Conoce usted alguna ley que penalice a quien o quienes cometan un delito informático?
    - ☐ Si
    - ☒ No

    Si su respuesta es "Si" mencione la ley : _____

GRACIAS POR SU COLABORACIÓN

3

Anexo 6: Resultados de la simulación

En la siguiente tabla se interpreta los resultados obtenidos en la herramienta Google Analytics (ver FIGURA 1), la cual permitió contabilizar los usuarios que fueron víctimas de la simulación realizada.

TABLA 1: *Interpretación de resultados de Google Analytics*

PAGINA	COD	GRUPO	ATAQUES ENVIADOS	ATAQUES CON EXITO	% ATAQUES CON EXITO
1	1004	C	1000	462	43,10
2	1001	A1	254	215	20,6
3	1005	D	1500	173	16,14
5	1002	A2	100	70	6,53
6	1003	B	110	34	3,17

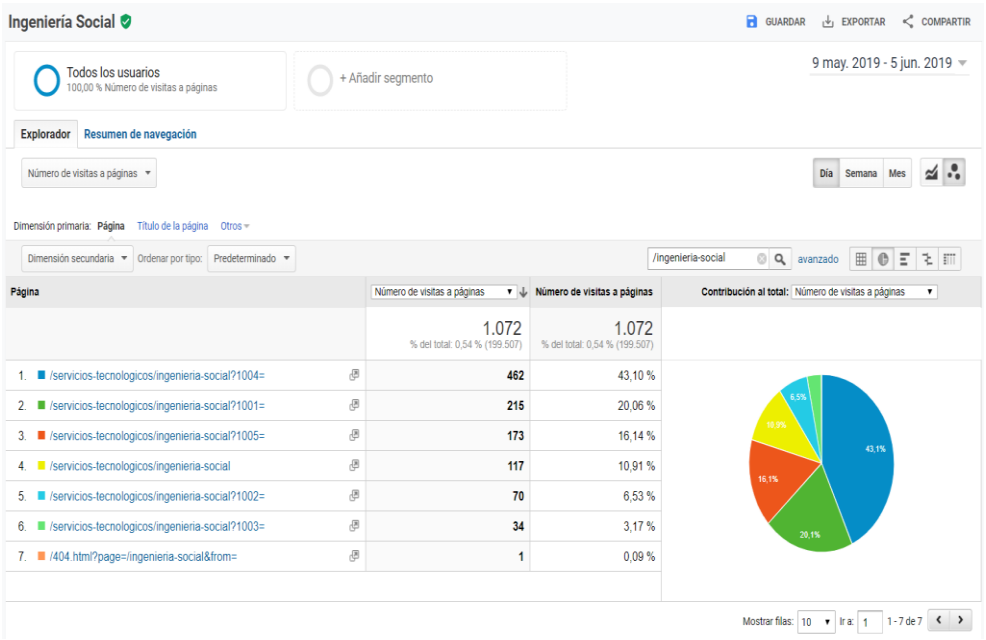
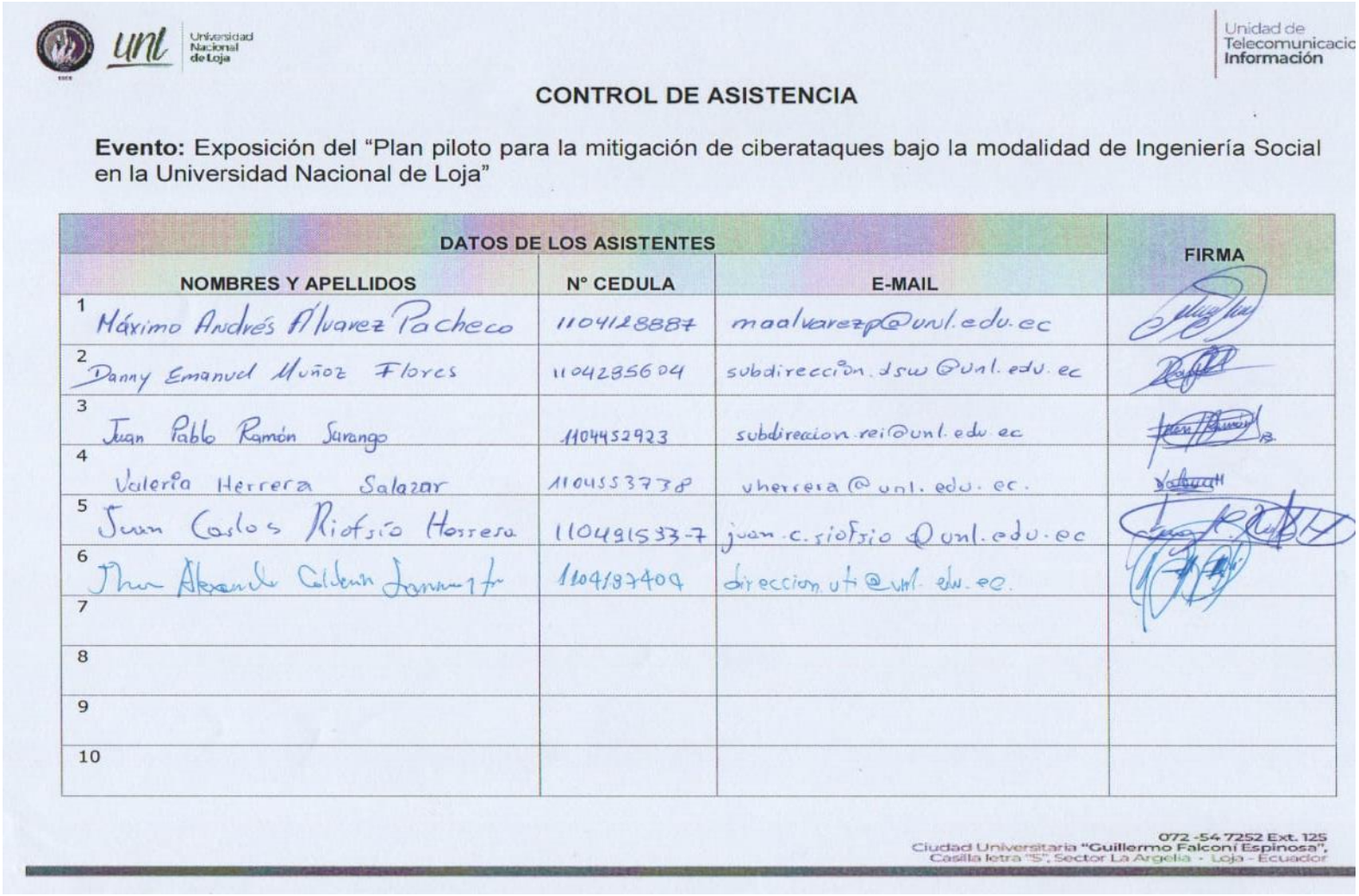


FIGURA 1: *Resultados de la simulación - Google Analytics*



Universidad Nacional de Loja

Unidad de Telecomunicacio Información

CONTROL DE ASISTENCIA

Evento: Exposición del "Plan piloto para la mitigación de ciberataques bajo la modalidad de Ingeniería Social en la Universidad Nacional de Loja"

	DATOS DE LOS ASISTENTES			FIRMA
	NOMBRES Y APELLIDOS	N° CEDULA	E-MAIL	
1	Máximo Andrés Alvarez Pacheco	1104128887	maalvarezp@unl.edu.ec	
2	Danny Emanuel Muñoz Flores	1104285604	subdireccion.dsw@unl.edu.ec	
3	Juan Pablo Ramón Surango	1104452923	subdireccion.rei@unl.edu.ec	
4	Valeria Herrera Salazar	1104553738	vherrera@unl.edu.ec.	
5	Juan Carlos Riofrío Herrera	1104915337	juan.c.riofrio@unl.edu.ec	
6	Juan Alexander Calderón Jaramillo	1104197404	direccion.uti@unl.edu.ec.	
7				
8				
9				
10				

072 -54 7252 Ext. 125
Ciudad Universitaria "Guillermo Falconí Espinosa",
Casilla letra "S", Sector La Argelia - Loja - Ecuador

Anexo 8: Control de cumplimiento

Universidad Nacional de Loja

Unidad de Telecomunicaciones e Información

CONTROL DE CUMPLIMIENTO

Fecha	15 de Agosto del 2019.
Autora	Srta. Jessica Pineda.
Tutora Académica	Ing. Valeria Herrera.
Tutor Técnico	Ing. Juan Carlos Riofrío.

En el siguiente documento se evalúa el cumplimiento de los aspectos que permitieron desarrollar el "Plan piloto para la mitigación de ciberataques bajo la modalidad de Ingeniería Social en la Universidad Nacional de Loja".

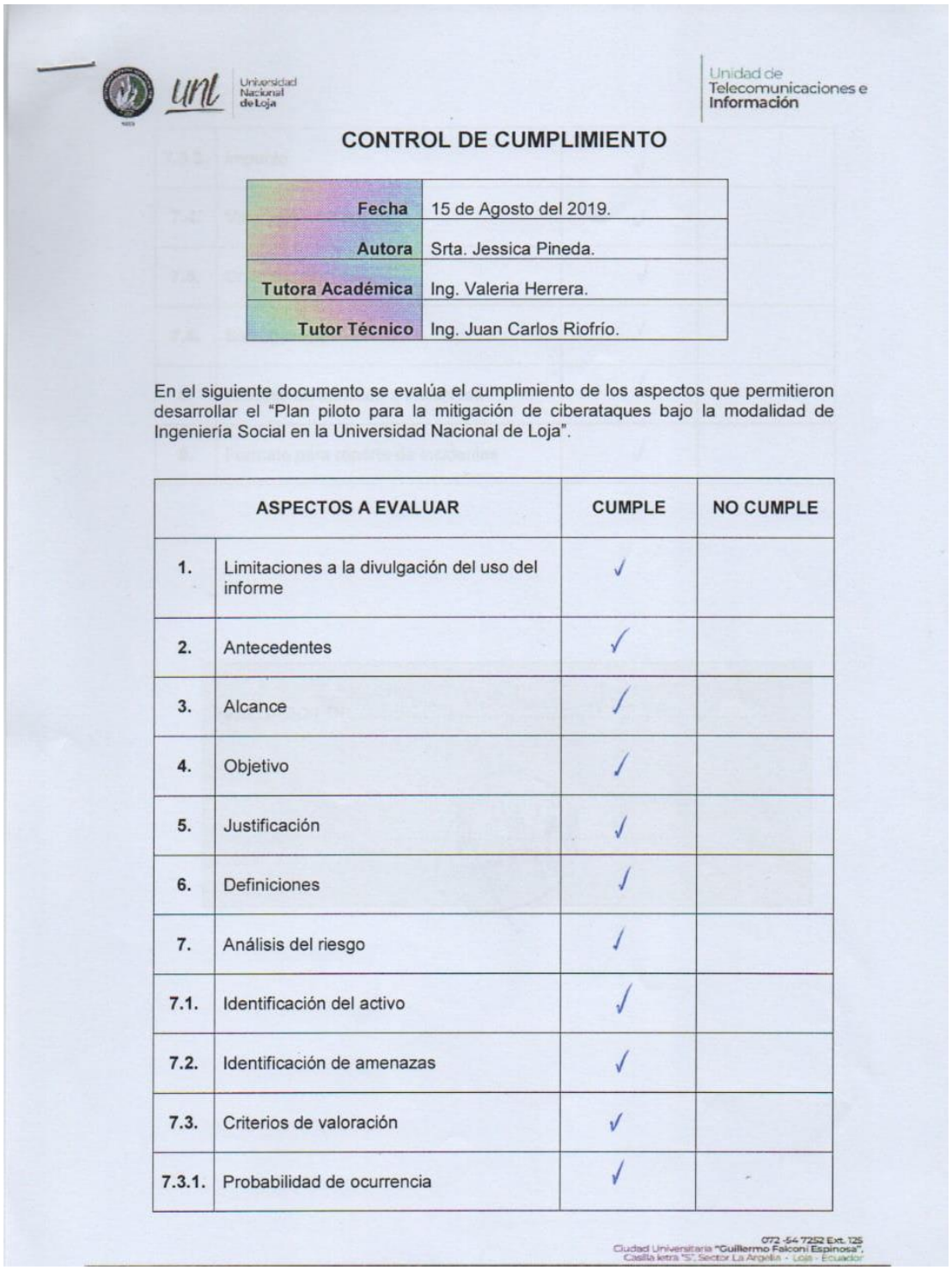
ASPECTOS A EVALUAR		CUMPLE	NO CUMPLE
1.	Limitaciones a la divulgación del uso del informe		
2.	Antecedentes		
3.	Alcance		
4.	Objetivo		
5.	Justificación		
6.	Definiciones		
7.	Análisis del riesgo		
7.1.	Identificación del activo		
7.2.	Identificación de amenazas		
7.3.	Criterios de valoración		
7.3.1.	Probabilidad de ocurrencia		

7.3.2.	Impacto		
7.4.	Valoración del riesgo		
7.5.	Criticidad del riesgo		
7.6.	Salvaguardias		
8.	Proceso de atención a incidentes		
9.	Formato para reporte de incidentes		

EVALUADO POR:.....

.....
FIRMA

Control de cumplimiento: Ing. Jhon Calderón



Universidad Nacional de Loja

Unidad de Telecomunicaciones e Información

CONTROL DE CUMPLIMIENTO

Fecha	15 de Agosto del 2019.
Autora	Srta. Jessica Pineda.
Tutora Académica	Ing. Valeria Herrera.
Tutor Técnico	Ing. Juan Carlos Riofrío.

En el siguiente documento se evalúa el cumplimiento de los aspectos que permitieron desarrollar el "Plan piloto para la mitigación de ciberataques bajo la modalidad de Ingeniería Social en la Universidad Nacional de Loja".

	ASPECTOS A EVALUAR	CUMPLE	NO CUMPLE
1.	Limitaciones a la divulgación del uso del informe	✓	
2.	Antecedentes	✓	
3.	Alcance	✓	
4.	Objetivo	✓	
5.	Justificación	✓	
6.	Definiciones	✓	
7.	Análisis del riesgo	✓	
7.1.	Identificación del activo	✓	
7.2.	Identificación de amenazas	✓	
7.3.	Criterios de valoración	✓	
7.3.1.	Probabilidad de ocurrencia	✓	

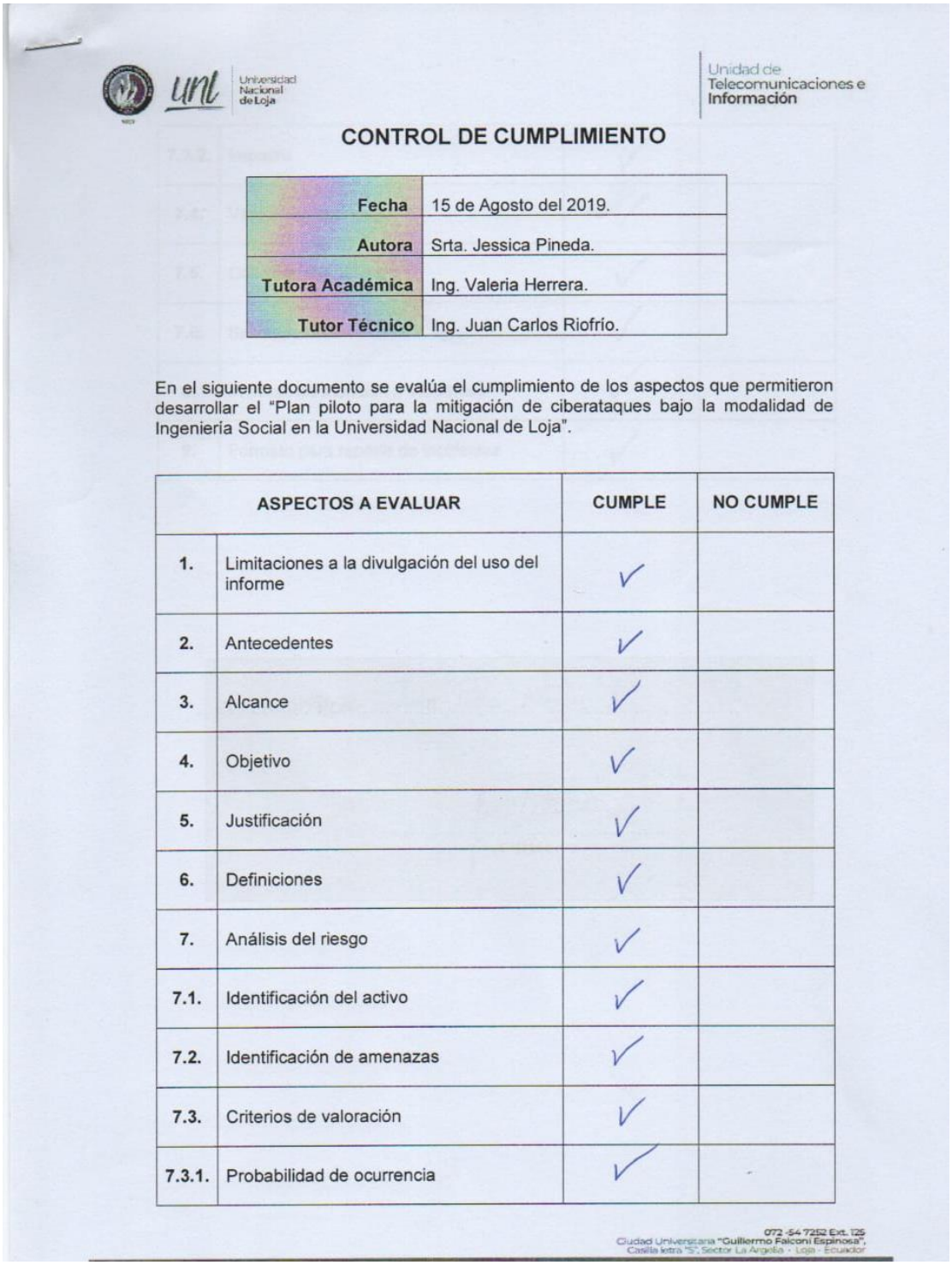
072 -54 7252 Ext. 125
Ciudad Universitaria "Guillermo Falconí Espinosa",
Casilla letra "S", Sector La Argelia - Loja - Ecuador

7.3.2.	Impacto	√	
7.4.	Valoración del riesgo	√	
7.5.	Criticidad del riesgo	√	
7.6.	Salvaguardias	√	
8.	Proceso de atención a incidentes	√	
9.	Formato para reporte de incidentes	√	

EVALUADO POR: Ing. Cristhian Sarmiento

FIRMA

Control de cumplimiento: Ing. Juan Pablo Ramón



Universidad Nacional de Loja

Unidad de Telecomunicaciones e Información

CONTROL DE CUMPLIMIENTO

Fecha	15 de Agosto del 2019.
Autora	Srta. Jessica Pineda.
Tutora Académica	Ing. Valeria Herrera.
Tutor Técnico	Ing. Juan Carlos Riofrío.

En el siguiente documento se evalúa el cumplimiento de los aspectos que permitieron desarrollar el "Plan piloto para la mitigación de ciberataques bajo la modalidad de Ingeniería Social en la Universidad Nacional de Loja".

	ASPECTOS A EVALUAR	CUMPLE	NO CUMPLE
1.	Limitaciones a la divulgación del uso del informe	✓	
2.	Antecedentes	✓	
3.	Alcance	✓	
4.	Objetivo	✓	
5.	Justificación	✓	
6.	Definiciones	✓	
7.	Análisis del riesgo	✓	
7.1.	Identificación del activo	✓	
7.2.	Identificación de amenazas	✓	
7.3.	Criterios de valoración	✓	
7.3.1.	Probabilidad de ocurrencia	✓	

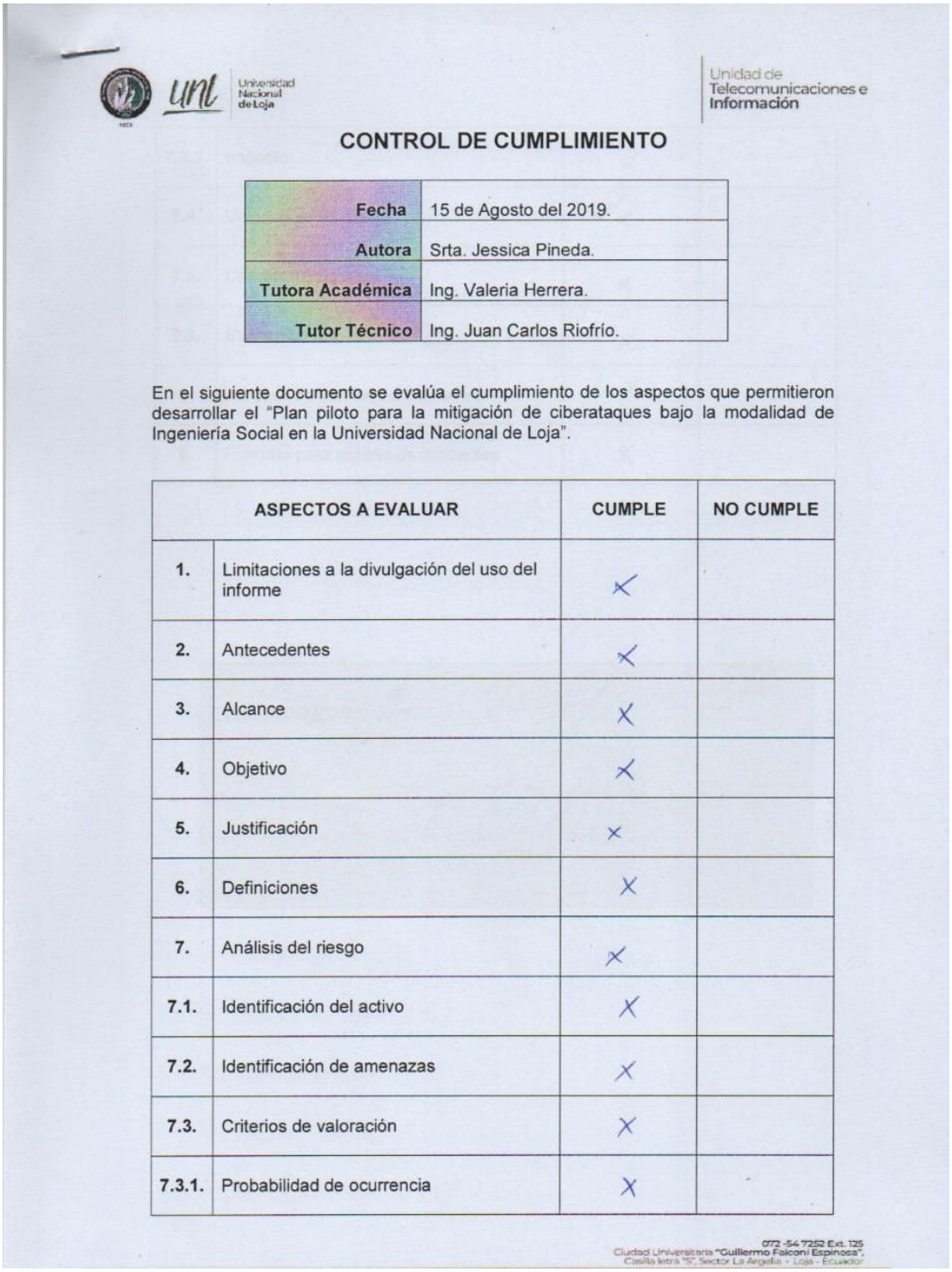
072 -54 7252 Ext. 125
Ciudad Universitaria "Guillermo Falconí Espinosa",
Casilla letra "S", Sector La Argelia - Loja - Ecuador

7.3.2.	Impacto	✓	
7.4.	Valoración del riesgo	✓	
7.5.	Criticidad del riesgo	✓	
7.6.	Salvaguardias	✓	
8.	Proceso de atención a incidentes	✓	
9.	Formato para reporte de incidentes	✓	

EVALUADO POR: Juan Pablo Ramón S.

FIRMA

Control de cumplimiento: Ing. Juan Carlos Riofrío



Universidad Nacional de Loja

Unidad de Telecomunicaciones e Información

CONTROL DE CUMPLIMIENTO

Fecha	15 de Agosto del 2019.
Autora	Srta. Jessica Pineda.
Tutora Académica	Ing. Valeria Herrera.
Tutor Técnico	Ing. Juan Carlos Riofrío.

En el siguiente documento se evalúa el cumplimiento de los aspectos que permitieron desarrollar el "Plan piloto para la mitigación de ciberataques bajo la modalidad de Ingeniería Social en la Universidad Nacional de Loja".

	ASPECTOS A EVALUAR	CUMPLE	NO CUMPLE
1.	Limitaciones a la divulgación del uso del informe	X	
2.	Antecedentes	X	
3.	Alcance	X	
4.	Objetivo	X	
5.	Justificación	X	
6.	Definiciones	X	
7.	Análisis del riesgo	X	
7.1.	Identificación del activo	X	
7.2.	Identificación de amenazas	X	
7.3.	Criterios de valoración	X	
7.3.1.	Probabilidad de ocurrencia	X	

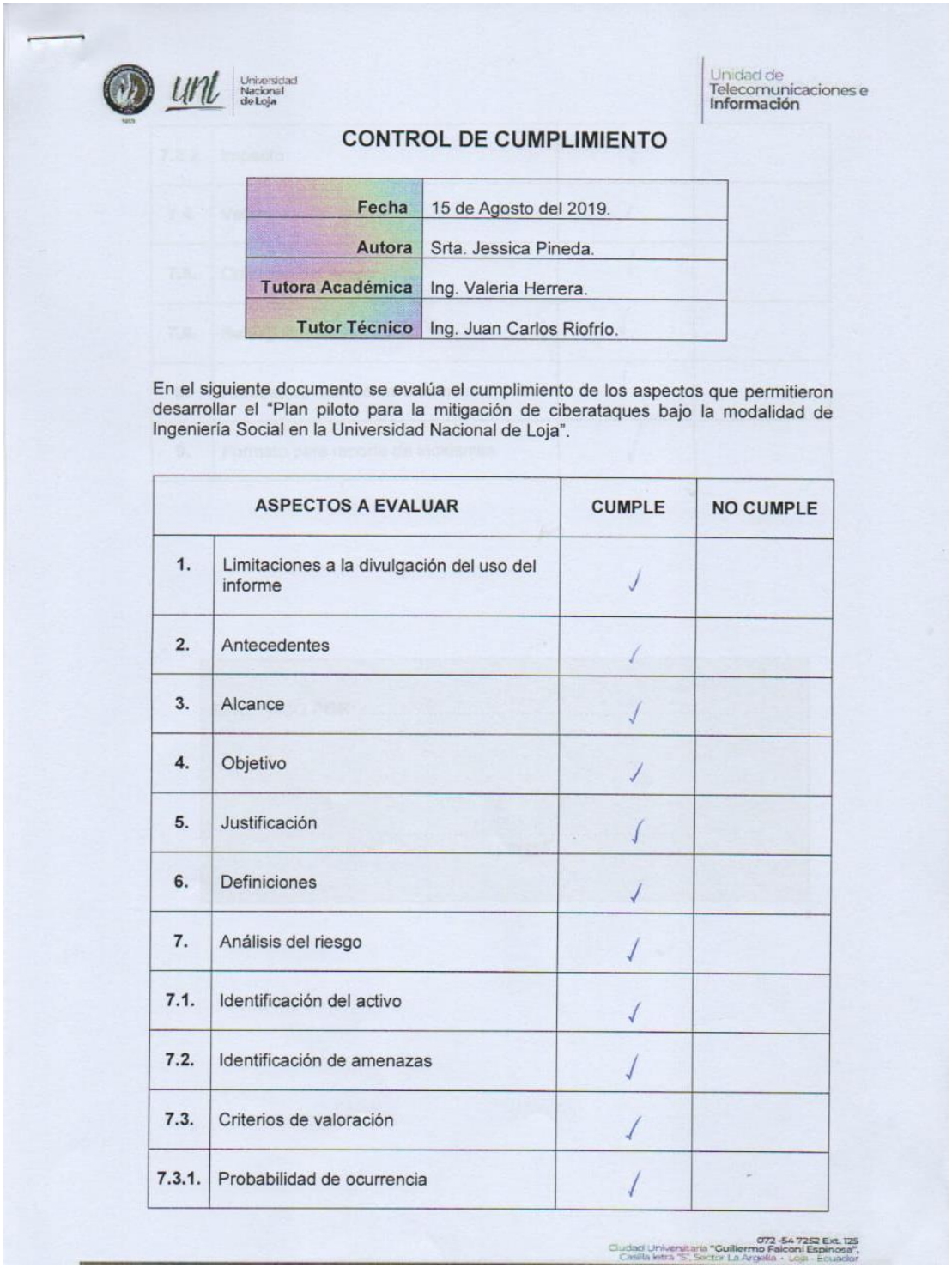
072 -54 7252 Ext. 125
Ciudad Universitaria "Guillermo Falconí Espinosa",
Casilla letra "S", Sector La Argelia - Loja - Ecuador

7.3.2.	Impacto	X	
7.4.	Valoración del riesgo	X	
7.5.	Criticidad del riesgo	X	
7.6.	Salvaguardias	X	
8.	Proceso de atención a incidentes	X	
9.	Formato para reporte de incidentes	X	

EVALUADO POR: Juan Carlos Ríofrío Herrera

FIRMA

Control de cumplimiento: Ing. Valeria Herrera



Universidad Nacional de Loja

Unidad de Telecomunicaciones e Información

CONTROL DE CUMPLIMIENTO

Fecha	15 de Agosto del 2019.
Autora	Srta. Jessica Pineda.
Tutora Académica	Ing. Valeria Herrera.
Tutor Técnico	Ing. Juan Carlos Riofrío.

En el siguiente documento se evalúa el cumplimiento de los aspectos que permitieron desarrollar el "Plan piloto para la mitigación de ciberataques bajo la modalidad de Ingeniería Social en la Universidad Nacional de Loja".

	ASPECTOS A EVALUAR	CUMPLE	NO CUMPLE
1.	Limitaciones a la divulgación del uso del informe	✓	
2.	Antecedentes	✓	
3.	Alcance	✓	
4.	Objetivo	✓	
5.	Justificación	✓	
6.	Definiciones	✓	
7.	Análisis del riesgo	✓	
7.1.	Identificación del activo	✓	
7.2.	Identificación de amenazas	✓	
7.3.	Criterios de valoración	✓	
7.3.1.	Probabilidad de ocurrencia	✓	

072 -54 7252 Ext. 125
Ciudad Universitaria "Guillermo Falconí Espinosa",
Casilla letra "S", Sector La Argelia - Loja - Ecuador

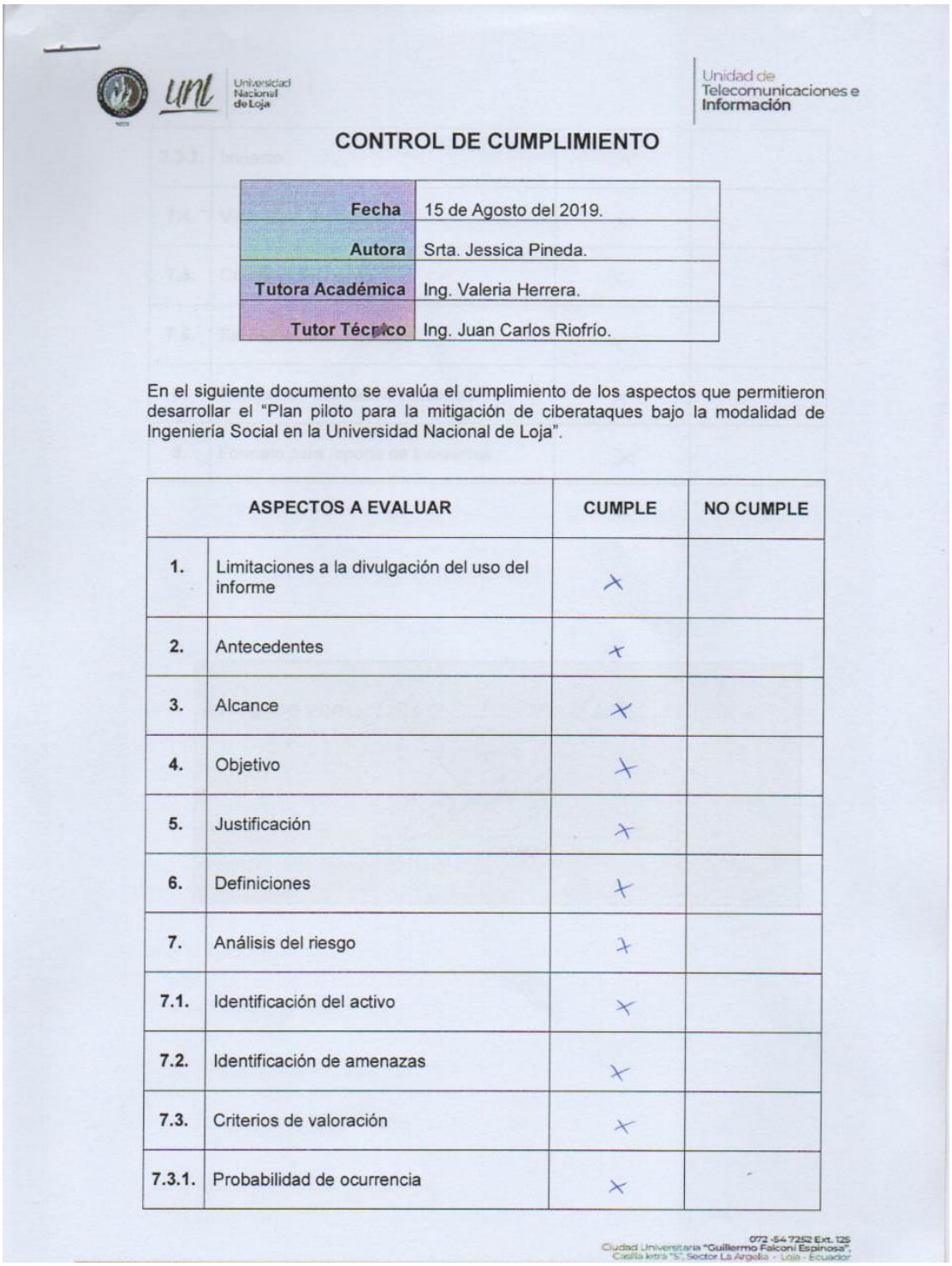
7.3.2.	Impacto	√	
7.4.	Valoración del riesgo	√	
7.5.	Criticidad del riesgo	√	
7.6.	Salvaguardias	√	
8.	Proceso de atención a incidentes	√	
9.	Formato para reporte de incidentes	√	

EVALUADO POR: Valeria Herrera Salazar.

.....

FIRMA

Control de cumplimiento: Ing. Máximo Álvarez



Universidad Nacional de Loja

Unidad de Telecomunicaciones e Información

CONTROL DE CUMPLIMIENTO

Fecha	15 de Agosto del 2019.
Autora	Srta. Jessica Pineda.
Tutora Académica	Ing. Valeria Herrera.
Tutor Técnico	Ing. Juan Carlos Riofrío.

En el siguiente documento se evalúa el cumplimiento de los aspectos que permitieron desarrollar el "Plan piloto para la mitigación de ciberataques bajo la modalidad de Ingeniería Social en la Universidad Nacional de Loja".

	ASPECTOS A EVALUAR	CUMPLE	NO CUMPLE
1.	Limitaciones a la divulgación del uso del informe	X	
2.	Antecedentes	X	
3.	Alcance	X	
4.	Objetivo	X	
5.	Justificación	X	
6.	Definiciones	X	
7.	Análisis del riesgo	X	
7.1.	Identificación del activo	X	
7.2.	Identificación de amenazas	X	
7.3.	Criterios de valoración	X	
7.3.1.	Probabilidad de ocurrencia	X	

072 -54 7252 Ext. 125
Ciudad Universitaria "Guillermo Falconi Espinosa".
Casilla letra "S", Sector La Argelia - Loja - Ecuador

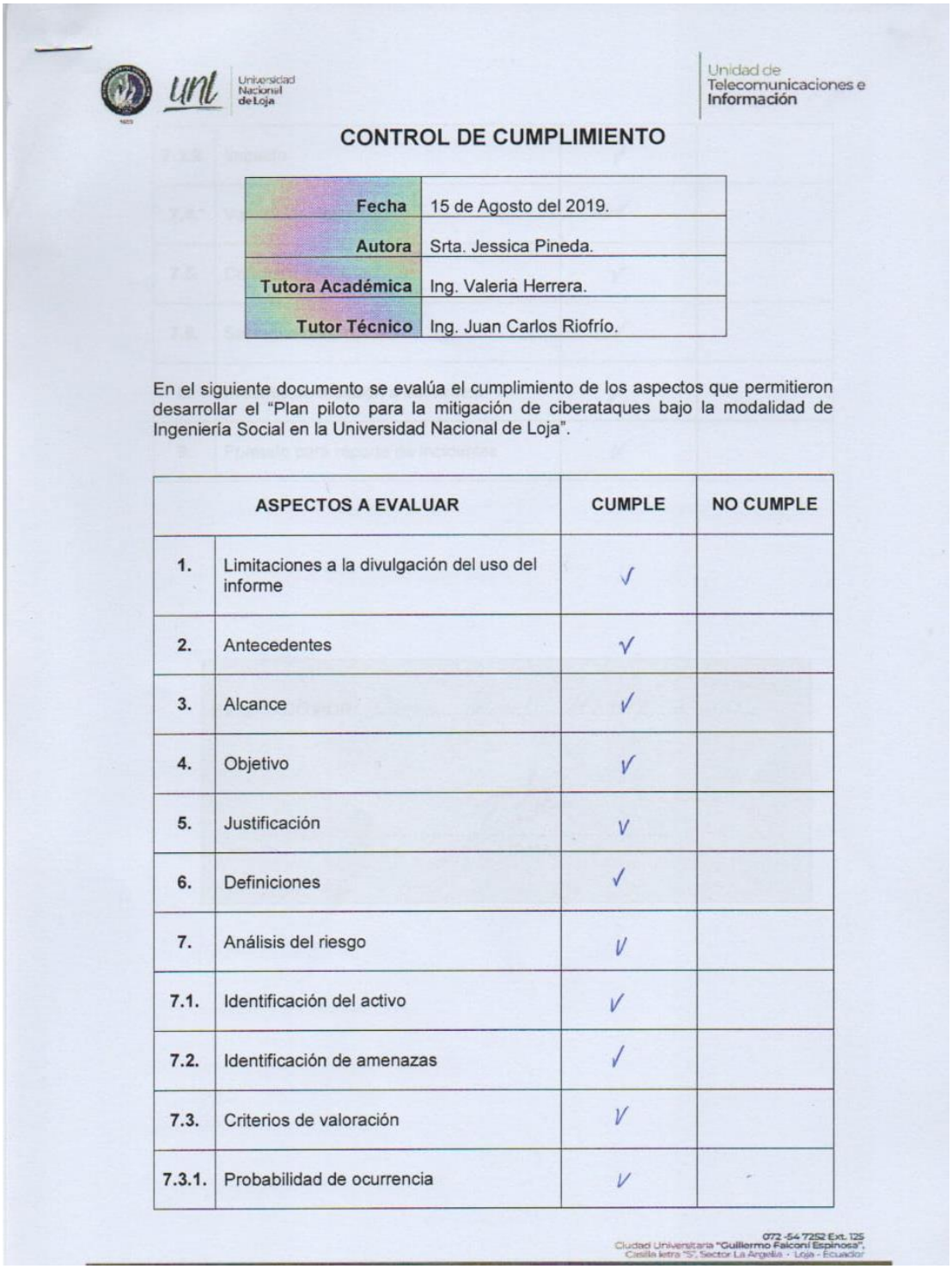
7.3.2.	Impacto	X	
7.4.	Valoración del riesgo	X	
7.5.	Criticidad del riesgo	X	
7.6.	Salvaguardias	X	
8.	Proceso de atención a incidentes	X	
9.	Formato para reporte de incidentes	X	

EVALUADO POR: Máximo Andres Alvarez Pacheco

.....

FIRMA

Control de cumplimiento: Ing. Danny Muñoz



Universidad Nacional de Loja

Unidad de Telecomunicaciones e Información

CONTROL DE CUMPLIMIENTO

Fecha	15 de Agosto del 2019.
Autora	Srta. Jessica Pineda.
Tutora Académica	Ing. Valeria Herrera.
Tutor Técnico	Ing. Juan Carlos Riofrío.

En el siguiente documento se evalúa el cumplimiento de los aspectos que permitieron desarrollar el "Plan piloto para la mitigación de ciberataques bajo la modalidad de Ingeniería Social en la Universidad Nacional de Loja".

	ASPECTOS A EVALUAR	CUMPLE	NO CUMPLE
1.	Limitaciones a la divulgación del uso del informe	√	
2.	Antecedentes	√	
3.	Alcance	√	
4.	Objetivo	√	
5.	Justificación	√	
6.	Definiciones	√	
7.	Análisis del riesgo	√	
7.1.	Identificación del activo	√	
7.2.	Identificación de amenazas	√	
7.3.	Criterios de valoración	√	
7.3.1.	Probabilidad de ocurrencia	√	

072 -54 7252 Ext. 125
Ciudad Universitaria "Guillermo Falconí Espinosa".
Casilla letra "S", Sector La Argelia - Loja - Ecuador

7.3.2.	Impacto	✓	
7.4.	Valoración del riesgo	✓	
7.5.	Criticidad del riesgo	✓	
7.6.	Salvaguardias	✓	
8.	Proceso de atención a incidentes	✓	
9.	Formato para reporte de incidentes	✓	

EVALUADO POR: Danny Emanuel Muñoz Flores

FIRMA

Anexo 9: Certificado de finalización del TT emitido por UTI.

Universidad Nacional de Loja

Unidad de Telecomunicaciones e Información

DIRECTOR DE TELECOMUNICACIONES E INFORMACIÓN

C E R T I F I C A:

Que la señorita Jessica Mariuxi Pineda Criollo con cédula de ciudadanía número 1104959547, egresada de la Carrera de Ingeniería en Sistemas, según los lineamientos y requerimientos de la UNIDAD DE TELECOMUNICACIONES E INFORMACIÓN, ha finalizado y entregado la documentación de su proyecto de titulación denominado: "*Plan piloto para la mitigación de ciberataques bajo la modalidad de Ingeniería Social en la Universidad Nacional de Loja*".

Es cuanto puedo indicar en honor a la verdad, facultando al interesado, hacer uso del presente documento.

Loja, 27 de septiembre de 2019

Jhon Alexander Calderón Sanmartín
DIRECTOR DE TELECOMUNICACIONES E INFORMACIÓN

UNL

072 -54 7252 Ext. 125
Ciudad Universitaria "Guillermo Falconí Espinosa",
Casilla letra "S" Sector La Argelia Loja Ecuador