****

Ética y Deontología Profesional

Proyecto de Responsabilidad Empresarial

**La Batalla de la Seguridad Digital: Protegiendo tu identidad en línea**

**Integrantes:**

Silvia Casermeiro

Angelo Menel

Santiago Vietto

**Profesora:** Lic. Schiavoni, Fernanda

**Índice**

| **1. Fundamentación de la propuesta**  **1.1. Marco teórico**  **1.2. Formulación del problema**  **2. Objetivos del proyecto**  **3. Beneficiarios de la propuesta**  **4. Agentes que intervienen en la propuesta**  **5. Plan de trabajo**  **6. Cronograma de actividades**  **7. Evaluación del proyecto**  **8. Comunicación del proyecto**  **9. Consideraciones finales**  **10. Bibliografía**  **11. Anexo**  **11.1. Anexo I**  **11.2 Anexo II** | **3**  **3**  **7**  **8**  **8**  **9**  **9**  **11**  **12**  **13**  **14**  **16**  **17**  **17**  **20** |
| --- | --- |

1. Fundamentos del proyecto

1.1 Marco teórico

Ubicándonos en esta era digital en la que vivimos, primero deberíamos definirla. ¿Qué es esta era digital? Podemos mencionar que *la norma ISO 27001 ofrece los requisitos necesarios para establecer un Sistema de Gestión de Seguridad de la Información en las organizaciones. En la actualidad, el término “ciberseguridad” se encuentra asociado a ciberespacio, ciberamenazas, etc*. Luego, nos gustaría mencionar que la seguridad digital y la protección de la privacidad se han vuelto de vital importancia. Podemos definir a *la ciberseguridad como la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos*. También se conoce como *seguridad de tecnología de la información o seguridad de la información electrónica*. Con respecto a la *privacidad en línea, ésta se centra en la protección de la información personal y en la capacidad de controlar quién accede a ella y cómo se utiliza*.



Como todos hoy en día, estamos constantemente conectados a través de dispositivos y aplicaciones en tiempo real, enviando y recibiendo información personal y realizando transacciones en línea. Sin embargo, no es del todo seguro. Las vulnerabilidades de la privacidad en línea pueden exponer a las personas a diversas amenazas, como el robo de identidad, el acoso cibernético, el fraude y la violación de la privacidad.

Las amenazas pueden manifestarse de diferentes formas, como el *phishing*, que consiste en engañar a las personas para que revelen información confidencial, o el *malware*, que es un software malicioso diseñado para dañar o acceder de manera no autorizada a los sistemas. Además, las *redes sociales* y las *aplicaciones en línea* también pueden dar lugar a que la privacidad se vea comprometida, ya que la información compartida puede ser utilizada sin el consentimiento de los usuarios.

Es muy importante comprender los riesgos y tomar medidas necesarias para protegerse mientras se está en internet. Algunas buenas prácticas, es utilizar contraseñas seguras, mantener el software antivirus actualizado, verificar con quién se comparte información personal, verificar la autenticidad de los sitios web y correos electrónicos, y configurar adecuadamente las opciones de privacidad en las redes sociales.

La seguridad digital y la protección de la privacidad son responsabilidades compartidas entre los usuarios, las organizaciones y los proveedores de servicios de internet. La educación y la sensibilización desempeñan un papel fundamental para capacitar a las personas en la adopción de prácticas seguras y en la comprensión de los riesgos asociados con la era digital.

Como estrategia para llevar a cabo esta campaña de sensibilización sobre la seguridad digital, no solo debemos concientizar sino también educar. Es por eso que a continuación, proponemos el flujo a seguir para lograrlo:

| **Campaña de sensibilización sobre la seguridad digital** | |
| --- | --- |
|  | Sensibilización: La sensibilización es hacer que se conozca el problema. La sensibilización no es igual a un conocimiento profundo. |
|  | Educación: La educación es la presentación de la información específica que el público necesita saber. |
|  | Conocimiento: El conocimiento se logra cuando se ha retenido el material educativo. |
|  | Habilidades: Las habilidades se construyen sobre el conocimiento adquirido, requieren práctica y se desarrollan con el tiempo. |
|  | Capacidad: La capacidad es poder llevar a cabo las habilidades necesarias para la destreza. |
|  | Hábito: El hábito se produce cuando las habilidades y conocimientos se ponen en práctica y se arraigan en la rutina diaria. |
|  | Cambio cultural: Un cambio cultural comienza a ocurrir cuando un número suficiente de personas han incorporado los buenos hábitos. |

Los Objetivos de Desarrollo Sostenible (ODS), también conocidos como Objetivos Globales, fueron adoptados por las Naciones Unidas en 2015 como un llamamiento universal para poner fin a la pobreza, proteger el planeta y garantizar que para el 2030 todas las personas disfruten de paz y prosperidad. Respecto a nuestro proyecto, podemos relacionarlo con las siguientes ODS:

* ODS 4: Educación de calidad - *la educación es uno de los motores más poderosos y probados para garantizar el desarrollo sostenible*. El proyecto se centra en la educación de personas en el manejo seguro de internet y la protección de datos. El fin es que las personas reciban una educación de calidad y conciencia sobre la seguridad en línea.
* ODS 9: Industria, innovación e infraestructura - *La inversión en infraestructura y la innovación son motores fundamentales del crecimiento y el desarrollo económico*. El proyecto menciona la necesidad de una infraestructura digital segura y fomentar la innovación en seguridad en línea. El fin es garantizar el acceso igualitario a la información y el conocimiento, obteniendo un entorno en línea más seguro y confiable.
* ODS 16: Paz, justicia e instituciones sólidas - *buscan reducir sustancialmente todas las formas de violencia y trabajan con los gobiernos y las comunidades para encontrar soluciones duraderas a los conflictos e inseguridad*. El fin es promover los derechos humanos relacionados a la seguridad digital y la protección de datos que son fundamentales para promover la paz, la justicia y el establecimiento de instituciones sólidas evitando el delito cibernético, el robo de identidad y otras violaciones de la privacidad.
* ODS 17: Alianzas para lograr los objetivos - *solo se pueden lograr con el compromiso decidido a favor de alianzas mundiales y cooperación*. El fin es fomentar la colaboración entre diferentes gobiernos, organizaciones de la sociedad civil y empresas, para promover la seguridad digital.

La Declaración Universal de los Derechos Humanos (DUDH) es un documento adoptado por la Asamblea General de las Naciones Unidas en su Resolución 217 A (III), el 10 de diciembre de 1948 en París,1​ que recoge en sus 30 artículos los derechos humanos considerados básicos niendo en cuenta los DDHH. Si nos enfocamos en nuestro proyecto, este se relaciona con aquellos derechos civiles y políticos fundamentales. Hemos listado los que consideramos relacionados a la campaña de seguridad digital y privacidad de los datos:

1. Art 3 - Derecho a la vida y la seguridad. Se busca la seguridad en línea, protegiendo la vida y la integridad de las personas en el entorno digital. Al educar a las personas sobre cómo mantenerse seguras en línea, se contribuye a garantizar su derecho a la vida y a vivir libres de amenazas y violencia.
2. Art 10 - Derecho a la igualdad ante la ley. Se busca educar a las personas de todas las edades, sin importar su origen, género o cualquier otra característica. Esto está alineado con el derecho a la igualdad ante la ley, que implica que todas las personas deben tener acceso a los mismos derechos y oportunidades sin discriminación.
3. Art 12 - Derecho a la privacidad. El objetivo es proteger la privacidad de las personas en línea, esto es, el derecho a proteger la información personal y controlar su divulgación.
4. Art 18 - Derecho a la libertad de expresión. Se busca garantizar que las personas puedan ejercer su derecho a la libertad de expresión sin temor a represalias o a violaciones de su privacidad.

1.2 Formulación del problema

La campaña de sensibilización sobre la seguridad digital busca resolver varios problemas relacionados con la falta de conciencia y conocimientos sobre cómo mantenerse seguros en línea y proteger los datos y la privacidad. Nosotros que hemos recibido ciertos conocimientos en la facultad acerca de los peligros que conlleva la conexión a internet y la realización de cualquier actividad, notamos ciertos inconvenientes que buscamos resolver.

Falta de conciencia sobre los riesgos: Muchas personas no son conscientes de los riesgos y peligros asociados con el uso de internet y las redes sociales. Esto puede llevar a una exposición involuntaria a estafas, malware, robo de identidad y otros ataques.

Buscamos ⇒ Aumentar la conciencia sobre estos riesgos y brindar información sobre cómo identificar y prevenir.

Desconocimiento de las prácticas de seguridad digital: Existe una falta de conocimiento generalizado sobre las mejores prácticas para mantenerse seguros en línea. Las personas pueden no saber cómo crear contraseñas seguras, reconocer correos electrónicos o sitios web falsos, o configurar adecuadamente la privacidad en las redes sociales.

Buscamos ⇒ Educar a las personas en estas prácticas esenciales de seguridad digital.

Vulnerabilidad de la privacidad y la protección de datos: Muchas personas no comprenden completamente cómo se recopila, utiliza y protege su información personal en línea. Esto puede llevar a una violación de la privacidad y al mal uso de los datos.

Buscamos ⇒ Informar a las personas sobre sus derechos de privacidad y proporcionarles herramientas y estrategias para proteger sus datos personales.

Falta de educación en seguridad digital: La educación en seguridad digital es escasa dejando a las personas sin las habilidades y conocimientos necesarios para protegerse adecuadamente en línea.

Buscamos ⇒ Promover la educación en seguridad digital desde una edad temprana.

Brecha generacional en la comprensión de la seguridad digital: Las personas mayores pueden enfrentar mayores desafíos en la comprensión y adopción de prácticas de seguridad digital.

Buscamos ⇒ Achicar esta brecha generacional y asegurar que las personas de todas las edades tengan acceso a la capacitación y la información necesaria para protegerse en línea.

1. **Objetivos del proyecto**

**Objetivos Generales:**

Promover la conciencia y el conocimiento sobre la seguridad digital y protección de datos y privacidad, capacitando a personas de todas las edades para que puedan adoptar prácticas seguras en línea contribuyendo a la garantía de los derechos humanos de 1ra y 2da Generación acerca de la privacidad, la protección de datos y la seguridad en el entorno digital, en línea con los Objetivos de Desarrollo Sostenible (ODS) de la Agenda 2030 de las Naciones Unidas, en particular el ODS 16: Paz, justicia e instituciones sólidas.

Contribuir a la política de RSE del Hotel Libertador capacitando al personal e implementando políticas de seguridad digital pudiendo expandir el campo de aplicación a otros hoteles.

**Objetivos específicos**

Aumentar el conocimiento del personal del Hotel Libertador, capacitando a las personas en las mejores prácticas de seguridad digital y enseñándoles a proteger su información personal, durante la temporada baja de 2024, con el fin de crear una cultura de seguridad digital en la comunidad y empoderar a las personas para protegerse y ayudar a otros en el entorno digital.

1. **Beneficiarios**

Beneficiarios directos: Los beneficiarios directos son el personal que administra el hotel y que tiene acceso a internet. Estos incluyen a los empleados que trabajan en la recepción, el departamento de reservas, el área administrativa y cualquier otro personal involucrado en las operaciones diarias del hotel. Al participar en la campaña de sensibilización sobre la seguridad digital, recibirán educación y conocimientos sobre cómo mantenerse seguros en línea y proteger los datos del hotel, lo que les permitirá tomar medidas proactivas para evitar riesgos y amenazas cibernéticas.

Beneficiarios indirectos: Los beneficiarios indirectos son el personal de la UECI que se especializa en la seguridad digital. Al participar en la campaña, podrán compartir su experiencia y conocimientos sobre seguridad digital con el personal del hotel. A su vez, nosotros, que hemos recibido cierta formación en la facultad, en la materia Seguridad y Auditoría, podremos repasar y poner en práctica nuestros conocimientos.

1. **Agentes que intervienen en la propuesta**

Para poder implementar la campaña de sensibilización sobre la seguridad digital podemos contar, primero, con los conocimientos adquiridos cuando cursamos la materia Seguridad y Auditoría, en donde explican los diferentes tipos de ataques cibernéticos y violaciones a la seguridad de los datos y privacidad como así también como protegernos..

También contamos con el soporte de la UECI (Unidad Ejecutora contra Ciberdelincuencia) que forma parte del Ministerio de Seguridad, Justicia y DDHH La Rioja.

1. **Plan de trabajo**

En la siguiente tabla, incluímos las actividades requeridas para llevar a cabo esta campaña. Tener en cuenta, que el orden de las actividades puede variar según las necesidades y recursos disponibles, y es importante adaptarlas a las características de la comunidad y los participantes involucrados en la campaña.

| # | Actividad | Responsable | Recursos |
| --- | --- | --- | --- |
| 1 | Revisión de los fines de la campaña y determinar el alcance de la misma | Todos | Realidad del Hotel y necesidades de seguridad |
| 2 | Preparación de la propuesta de campaña | Todos | Presentación PP  Propuesta en Word |
| 3 | Presentar la propuesta de la campaña a la Gerencia del Hotel | Todos | Videollamada  Presentación PP  Propuesta en Word |
| 4 | Estudio del conocimiento sobre seguridad digital del Personal del hotel | Silvia Casermeiro | Encuestas y cuestionarios |
| 5 | Desarrollo de materiales educativos | Angelo Menel | Folletos  Power Point |
| 6 | Horarios y duración de talleres y charlas | Silvia Casermeiro | Días, horas y duración de cada encuentro |
| 7 | Buscar y preparar el lugar en donde se realizarán las capacitaciones | Santiago Vietto | Comunicación con el personal del hotel |
| 8 | Acondicionado del lugar de las capacitaciones | Santiago Vietto | Comunicación con el personal del hotel |
| 9 | Diseño de flyers y posters | Angelo Menel | Flyers y pósters |
| 10 | Comunicación de la campaña | Silvia Casermeiro | Whatsapp  Pósters |
| 11 | Dictar las capacitaciones | Todos | Power point  Folletos |
| 12 | Evaluación de contenidos aprendidos | Todos | Google forms |
| 13 | Soporte a incidentes | Todos | Recepción de email/sms por comportamientos sospechosos |
| 14 | Determinación de seguimiento dentro de los próximos 6 meses | Todos | Documento Word |

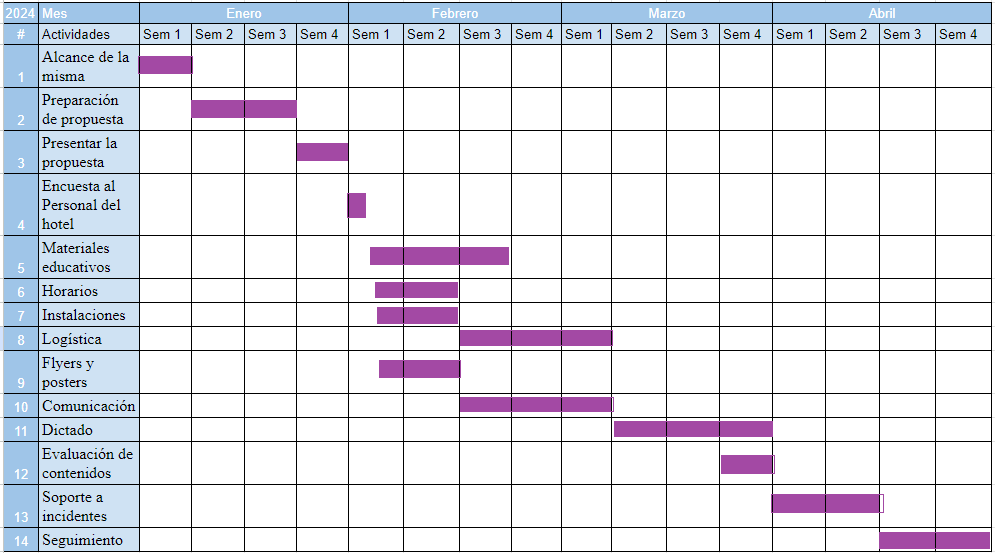
Folletos

Hemos preparado un esbozo de folleto que podríamos entregar como ayuda memoria para cada una de las personas que asistan a nuestras charlas con el propósito de tener a mano las buenas prácticas sobre seguridad digital.



1. **Cronograma de actividades**

A continuación, mostramos el desarrollo de todas las actividades relacionadas con la campaña. Hemos tenido en cuenta la temporada baja del hotel para poder tener la mayor participación.



1. **Evaluación del proyecto**

Para evaluar el éxito de la campaña de sensibilización sobre la seguridad digital y la efectividad de la capacitación proporcionada, se pueden utilizar varios indicadores y métodos de evaluación. Algunas formas de evaluar el éxito de la campaña pueden incluir:

Encuestas y/o cuestionarios: Realizar encuestas antes y después de la campaña para evaluar el conocimiento y la conciencia de seguridad digital de los participantes para medir el aumento en el conocimiento y la adopción de las buenas prácticas después de la capacitación.

Pruebas de conocimientos: Realizar breves exámenes para evaluar la comprensión y retención de la información por parte de los participantes. Se pueden proponer temas clave como generar contraseñas seguras, cómo proteger los datos y prevenir algún ataque cibernético.

Retroalimentacióndelpersonal: Hablar con el personal y recopilar comentarios y opiniones sobre la utilidad y relevancia de la capacitación. Esto sirve a la hora de aplicar posibles mejoras y conocer qué tan efectiva fue la campaña en términos de cambios de comportamiento y conciencia.

Seguimientodeincidentesdeseguridad: Hacer seguimiento de cualquier incidente de seguridad que ocurra antes y después de la campaña. Comparar los datos para evaluar si ha habido una disminución en los incidentes y una mayor capacidad de respuesta frente a las amenazas.

1. **Comunicación del proyecto**

El flyer que hemos diseñado, se colocará en los puntos estratégicos en donde los empleados puedan verlo.



Por el grupo de Whatsapp de los empleados, enviaremos el cronograma de charlas. El siguiente, sería un ejemplo de comunicación de cada encuentro.



Por cuestiones administrativas del hotel, se necesitará presentar a todos los empleados, el cronograma completo de actividades relacionadas a nuestra campaña. El siguiente póster será presentado y colocado en un lugar visible para todos los empleados.



Notar que los temas mencionados arriba son a título ilustrativo.

1. **Consideraciones finales**

Consideramos que es muy importante que las personas tomen conciencia de todos los riesgos que implican estar en línea. La tecnología continúa avanzando y nuestras vidas se vuelven cada vez más digitalizadas: compras on-lines, reservas on-line, transferencias bancarias, publicaciones en redes sociales. Nuestra campaña tiene como objetivo educar a personas de todas las edades sobre cómo mantenerse seguras en línea y proteger sus datos y privacidad.

Si lo vemos en términos de ética cívica, la implementación de esta campaña es esencial. La ética cívica se refiere a la responsabilidad y el comportamiento ético de los individuos en su vida cívica y en la sociedad en general. En el mundo digital, la ética cívica implica el respeto y la protección de la privacidad de los demás, el uso responsable de la información personal y la adhesión a las normas y leyes digitales. Con nuestra campaña de sensibilización sobre la seguridad digital, estaremos contribuyendo a la ética cívica al educar a las personas sobre sus derechos y responsabilidades en línea, fomentando el respeto mutuo y promoviendo comportamientos éticos en el internet.

Si hablamos de los valores que promueve esta campaña, podemos comenzar mencionando la Conciencia acerca de los riesgos y amenazas en línea y las malas prácticas llevadas a cabo por cada uno dando lugar al robo de identidad y violación de privacidad. Así, contribuiremos al bienestar colectivo y respeto mutuo cuando estemos en línea.

El siguiente valor que queremos mencionar es la Educación. Comunicando las buenas prácticas para mantenerse seguros en internet y proteger los datos y privacidad, como contraseñas seguras, identificación de sitios web y correos electrónicos sospechosos y una adecuada configuración de la privacidad en las redes sociales, ayudamos a las personas a que tomen decisiones éticas en línea.

Continuando con el valor de la Colaboración entre las personas, buscamos crear una comunidad, primero, a nivel empresarial, y luego social, a través de la comunicación abierta e intercambio de conocimientos y experiencias relacionadas con la seguridad en línea.

Por último, tener una Responsabilidad individual y colectiva es esencial. Cada persona debe ser responsable de proteger sus datos y privacidad y respetar los derechos y privacidad de los demás. Esto se puede lograr actualizando constantemente el software antivirus, usar contraseñas seguras y no compartirlas, tampoco compartir datos confidenciales en línea siendo siempre conscientes de lo que implican nuestras acciones en los demás.

En conclusión, la implementación de la campaña de sensibilización sobre la seguridad digital es fundamental para el futuro de las personas, tanto fuera como dentro del hotel. Buscamos concientizar sobre la conciencia, la educación, la colaboración y la responsabilidad. Si bien abarcamos un universo pequeño, el de los empleados del hotel, la idea es poder expandir estos conocimientos y que muchas más personas estén más al tanto de los peligros que corren al estar desprotegidos cuando están conectados a su redes sociales o hacen transacciones on line. Lamentablemente, no todos son éticos y se aprovechan de la falta de conocimiento de aquellos desprevenidos para ser blanco de fraudes o robo de identidad. Mientras más seamos los que conocemos y protegemos nuestros datos, protegemos a los otros y entre nosotros para, luego, poder llegar a una sociedad digital segura y ética.

1. **Bibliografía**

<https://www.studocu.com/es-mx/document/best-notes-for-high-school-mx/fundamentos-de-investigacion/marco-teorico-sobre-la-ciberseguridad-en-las-redes-sociales-y-su-importancia/18660818>

<https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2015%20OEA%20-%20Ciberseguridad%20Kit%20de%20Herramientas%20para%20la%20Campa%C3%B1a%20de%20Concientizaci%C3%B3n%20(Espa%C3%B1ol).pdf>

<https://www.undp.org/es/sustainable-development-goals>

<https://www.un.org/es/about-us/universal-declaration-of-human-rights>

<https://www.facebook.com/UeciLaRioja/>

<https://www.clarin.com/opinion/ciberseguridad-preocupante-situacion-argentina_0_g68YkgWvuo.html>

<https://www.iproup.com/innovacion/37754-la-seguridad-en-la-era-digital>

<https://www.perfil.com/noticias/economia/todo-lo-que-hay-que-saber-sobre-la-nueva-ley-de-proteccion-de-datos-personales.phtml>

1. **Anexo**

11.1. Anexo I

**La Batalla de la Seguridad Digital: Protegiendo tu identidad en línea**

Capacitación sobre cómo mantenerse seguro en internet protegiendo su privacidad

**Integrantes:**

Santiago Vietto, Angelo Menel, Silvia Casermeiro



**Objetivos Generales**

* Promover la conciencia y el conocimiento sobre la seguridad digital y protección de datos y privacidad, capacitando a personas de todas las edades para que puedan adoptar prácticas seguras en línea contribuyendo a la garantía de los derechos humanos de 1ra y 2da Generación acerca de la privacidad, la protección de datos y la seguridad en el entorno digital, en línea con los Objetivos de Desarrollo Sostenible (ODS) de la Agenda 2030 de las Naciones Unidas, en particular el ODS 16: Paz, justicia e instituciones sólidas.
* Contribuir a la política de RSE del Hotel Libertador capacitando al personal e implementando políticas de seguridad digital pudiendo expandir el campo de aplicación a otros hoteles.

**Objetivos específicos**

* Aumentar el conocimiento del personal del Hotel Libertador, capacitando a las personas en las mejores prácticas de seguridad digital y enseñándoles a proteger su información personal, durante la temporada baja de 2024, con el fin de crear una cultura de seguridad digital en la comunidad y empoderar a las personas para protegerse y ayudar a otros en el entorno digital.

**Beneficiarios**

*Directos*: Personal afectado que tenga acceso a internet y administren el hotel

*Indirectos*: La UECI y nosotros al especializarnos en la seguridad digital

**Resumen del proyecto**

La campaña de sensibilización sobre la seguridad digital es un proyecto que tiene como objetivo capacitar a personas de todas las edades en el manejo seguro de internet y la protección de sus datos y privacidad en línea.

El proyecto se enfoca en brindar información clara y concisa sobre los peligros potenciales asociados con el uso de internet y las redes sociales, así como en capacitar a las personas en la adopción de medidas de seguridad adecuadas. Esto incluye enseñar sobre el uso de contraseñas seguras, la identificación de sitios web y correos electrónicos fraudulentos, y la gestión adecuada de la configuración de privacidad en las redes sociales.

**Ejes o valores del proyecto**

* Conciencia: sobre los riesgos y amenazas en línea.
* Educación: capacitar sobre mejores prácticas para mantenerse seguros en línea y proteger los datos y la privacidad.
* Colaboración: crear una comunidad consciente de la seguridad digital
* Responsabilidad: individual y colectiva en el entorno digital sobre la toma de medidas proactivas para proteger los datos personales y la privacidad.

**Organización que participa**

Hotel Libertador, La Rioja, Argentina

UECI - Unidad Ejecutora contra Ciberdelincuencia del Ministerio de Seguridad, Justicia y DDHH La Rioja

11.2. Anexo II

**Nombre de la organización**

Hotel Libertador

**Bien interno de la organización**

**Misión**

Su misión es brindar a sus pasajeros una experiencia inolvidable, ofreciendo un ambiente acogedor, servicios de calidad y atención personalizada comprometiéndose a proporcionar un alojamiento confortable y servicios excelentes que superen las expectativas de sus huéspedes.

**Objetivos**

Su objetivo es crear un ambiente cálido y familiar donde los pasajeros se sientan bienvenidos y disfruten de su estadía en La Rioja, brindándoles comodidad, tranquilidad y una atención personalizada para garantizar una experiencia única y satisfactoria.

**Ubicación**

Buenos Aires 256, La Rioja capital, La Rioja, Argentina

****

**Facebook**

<https://www.facebook.com/libertadorhotellar/?locale=es_LA>

**Tamaño**

10 empleados

**Mapa de stakeholders**

