AJEA - Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1146.2022

Los recursos humanos como eje fundamental en la mitigación de riesgos de seguridad de la información en las organizaciones

Autores
Fabbri, Lucía Morena; Dolan, Guillermo
Departamento de Ingeniería en Sistemas de Información
Facultad Regional Rosario - Universidad Tecnológica Nacional
E. Zeballos 1341, 2000 Rosario, Argentina
fabbriluciam@gmail.com

Resumen

Este trabajo se orienta a analizar mecanismos de prevención de fuga de datos (Data Leakage Prevention) cuando los riesgos ya se han identificado y mecanismos de prevención de pérdida de datos (Data Loss Prevention) para mitigar dicha pérdida una vez que el riesgo se ha materializado. Con el fin de relacionar los términos de Data Leakage, Data Breach y Data Loss y analizar en contexto la inteligencia de amenazas se expondrán escenarios probables en cualquier organización de hoy en día. La exposición de un ejemplo de ataque permitirá analizar en contexto la inteligencia que estas amenazas ponen en juego.

Palabras clave: *Data Leakage, Data Breach, Data Loss, Zero Trust*

1. Introducción

Al momento de analizar los activos más importantes de una organización lo primero en lo que pensamos es en su capital financiero y el capital invertido en infraestructura, pero no podemos olvidarnos de las personas que sostienen los procesos de la organización y son quienes toman decisiones en base al los datos recolectados de fuentes tanto externas como internas con el propósito de mantener a los procesos operativos.

Se considera que en las organizaciones el factor humano es determinante en los ciberataques, que deben ser prevenidos y detectados en forma temprana.

Este factor debe ser analizado del lado del atacante, de la víctima o de ambos, identificando vulnerabilidades y amenazas que configurarán potenciales riesgos relacionados a los comportamientos humanos mientras realizan las actividades que contribuyen con un proceso organizacional.

Es por esto que en las organizaciones el factor humano es determinante en los ciberataques, ya que las personas no solo acceden a los datos diariamente para el desempeño de sus tareas, sino que también son un factor fundamental a la hora de detectar y prevenir este tipos de ataques de forma temprana, permitiendo de esta manera actuar en consecuencia antes de que los posibles daños sean mayores a los que la organización pueda soportar. Las herramientas tecnológicas son aliadas al momento de reducir la probabilidad de ocurrencia y el impacto que pueda tener un ciberataque.

[1]

Nuestro trabajo se basa en exponer la extrema responsabilidad que tiene el factor humano de la organización ante los ataques a la seguridad de la información, aun habiéndose implementado estrategias de mitigación del riesgo con herramientas tecnológicas y siguiendo buenas prácticas que se ajustan a las diferentes normas y estándares de seguridad vigentes.

De todos modos, las tecnologías no pueden por si mismas acaparar todas los aspectos que suponen las amenazas y las personas no sólo tienen que ser capacitadas para detectar estos ataques, sino que la información recolectada por estas herramientas debe ser correlacionada y así retroalimentar el conocimiento de la organización en cuanto a las amenazas que potencialmente se enfrentará en un futuro y así establecer el proceso de inteligencia contra amenazas.

En particular nos enfocaremos a la exposición de datos sensibles que maneja la organización en sus operaciones diarias, la filtración de datos y la pérdida de datos originando una violación a las normas de seguridad vigentes en cuanto a confidencialidad de datos, tanto en Argentina la Ley 25.326 de Protección de datos Personales como la actual Regulación de Protección de Datos Europea (GDPR), o impidiendo a la organización la continuidad de negocio.

AJEA - Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1146.2022

2. Exposición de Datos sensibles

Data Leakage es el concepto utilizado para definir cuando datos sensibles son expuestos y no supone un ciberataque sino la vulnerabilidad a la que se exponen los datos cuando no se cuenta con mecanismos y herramientas de seguridad o a partir de una falla humana. [2]

2.1. Tipos de Data Leakage y principales causas

Existen diversos tipos de exposición de datos sensibles:

1. **Violación accidental**: Accidentalmente un agente interno de la organización expone los datos a agentes externos a la misma vulnerando la confidencialidad de los mismos.
2. **Violación intencionada**: Un agente interno de la organización filtra intencionalmente datos de la organización con algún motivo asociado.
3. **Violación por negligencia**: Un agente interno que actúa de forma descuidada o por falta de conocimiento.

Entre las causas más comunes de Data Leakage se encuentran: [3]

1. Mala configuración de software o software desactualizado.
2. Ingeniería social
3. Reutilización de contraseñas
4. Robo de dispositivos físicos con datos sensibles
5. Vulnerabilidades de seguridad en el software
6. Utilizar contraseñas por default

Uno de los ejemplos que relacionan las categorías enunciadas es el phishing, que cae dentro de Ingeniería social y es del tipo violación por negligencia. Este puede originarse en comunicaciones electrónicas con intención maliciosa ya que el simple hecho de hacer clic en un enlace y visitar una página web que contiene un código malicioso podría permitir que el atacante acceda a una computadora o red, tomar el control y vulnerar los datos. Otro posible caso es la suplantación de identidad por medio de robo de dispositivos físicos o credenciales que permitan el acceso a la organización simulando ser un agente interno o con permiso de acceso.

3. Filtración de datos

Se denomina Data Breach o filtración de datos cuando una parte no autorizada accede a información confidencial o los ciberdelincuentes la roban aprovechando el Data Leakage.

3.1. Algunos datos interesantes referidos a Data Breach

En 2022 se alcanzó un récord histórico de 4,35 millones de dólares acorde a un estudio de IBM y el instituto Ponemon[4].

Este informe tiene en cuenta como factores de costo: actividades legales, reglamentarias y técnicas, pérdida de valor de marca, rotación de clientes y pérdida de productividad de los empleados.

Sus hallazgos se basan en 550 infracciones en 17 países y 17 industrias con datos recopilados de más de 3600 entrevistas

Los vectores de ataque comunes fueron:

- Las credenciales robadas o comprometidas fueron responsables del 19 % de las infracciones.
- El phishing fue responsable de las infracciones el 16 % de las veces.
- La mala configuración de la nube causó el 15 % de los ataques.

4. Pérdida de Datos confidenciales

Se denomina Data Loss cuando los datos confidenciales se extravían y no se pueden recuperar, ya sea a partir de robo a través de ataques cibernéticos o amenazas internas ocurridas en un Data Breach.

5. Buenas prácticas para hacer frente a las amenazas expuestas

5.1. Zero Trust

El modelo Zero Trust se basa en el paradigma “Nunca confiar, siempre verificar” y cuenta con cinco principios básicos.

- Siempre se presupone que todos los usuarios de una red son hostiles.
- Existen amenazas externas e internas en la red en todo momento.
- La localización de la red no es suficiente para decidir su nivel de confianza.
- Cada dispositivo, usuario y flujo de red se autentica y autoriza.
- Las políticas deben ser dinámicas y se deben calcular a partir de tantas fuentes de datos como sea posible.

AJEA - Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1146.2022

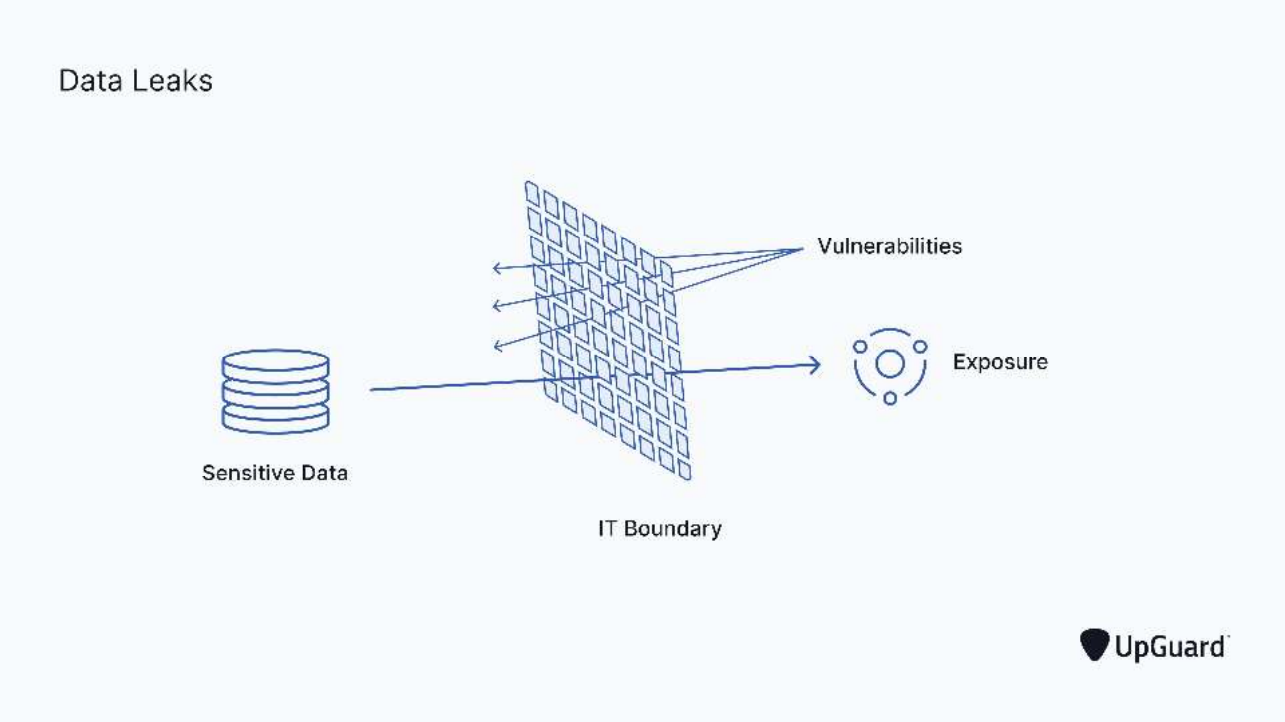

Figura 1. Data Leakage

Cada vez son más las organizaciones que adoptan un modelo de seguridad zero trust.

La proporción de organizaciones que implementan Zero Trust creció del 35 % en 2021 al 41 % en 2022 [4].

Las organizaciones que no implementan Zero Trust incurrieron en un promedio de USD 1 millón más en costos por incumplimiento en comparación con aquellas que implementan Zero Trust.

6. Data Loss Prevention

Data Loss Prevention (Data Loss Prevention) abarca una serie de estrategias de seguridad de la información para que la misma pueda ser transmitida o intercambiada dentro de los límites establecidos en las normas de seguridad de la organización.

Para cumplir con la Regulación General de Protección de Datos Europea (GDPR), las empresas deben estar al tanto de los incidentes de violación de datos inmediatamente después de que ocurran para que puedan tomar medidas inmediatas.

La GDPR responsabiliza legalmente a las empresas por la pérdida de datos o los incidentes de filtración de datos. Las soluciones de Data Loss Prevention permiten cumplir con las consideraciones impuestas por la GDPR. Entre estas consideraciones podemos mencionar:

- Capacidad de encontrar automáticamente información de identificación personal (PII) en función de condiciones y reglas de detección predefinidas y personalizables.
- Detección de las infracciones a la GDPR y falta de cumplimiento de las políticas de seguridad de datos a través del cifrado de los mismos, enviando alertas para ayudar a los administradores a tomar medidas correctivas cuando sea necesario.
- Determinación del flujo y trayecto de datos entre los usuarios de una organización y los externos a la misma que sean permitidos (Trazabilidad).
- Conocimiento por parte de los controladores y procesadores de datos del lugar donde se almacena o procesa la información personal, permitiendo a los administradores escanear todas las flotas de dispositivos y computadoras para detectar datos que se han marcado como çonfidenciales"según las políticas de la organización y las reglas de cumplimiento con la GDPR.
- Generación de informes a la Agencia de Protección de Datos (DPA) a pedido.

AJEA - Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1146.2022

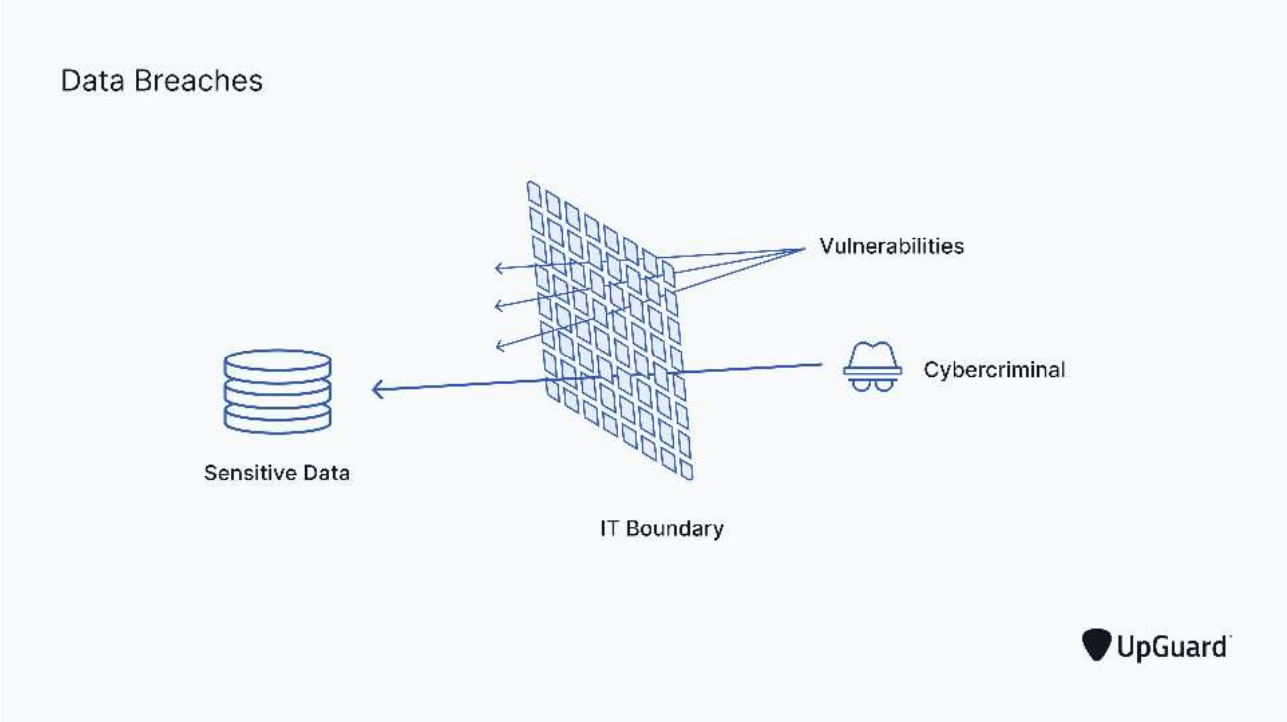

Figura 2. Data Breach

- Garantía de que los datos personales no se utilicen para ningún otro propósito que no sea para el que se suponía que debían ser utilizados. En este sentido las tecnologías Data Loss Prevention restringen la carga, impresión o copia y pegado de datos personales e imponen restricciones para cargar datos en dispositivos personales o servicios en la nube aplicando políticas para restringir la transferencia de datos no autorizada tanto fuera como dentro de la organización, permitiendo además a los administradores de TI monitorear fácilmente los datos en uso.
- Eliminación de datos no necesarios ya sea en forma local o remota, y en forma de cifrando o eliminación física.

6.1. Normas Internacionales de seguridad de la Información

La Familia de Normas ISO 27000 [5], donde la última versión certificable es la ISO 27001:2013 (con correcciones al 2015), propone un marco para el Sistema de Gestión de la Seguridad de la Información (SGSI), que permite coordinar la definición de políticas, objetivos y alcance de la seguridad de la información en la organización, el análisis, valorización y tratamiento de los riesgos sobre los activos involucrados, los controles a realizar y su monitorización para luego efectuar las mejoras correspondientes. La implementación de esta Norma permite cumplir con la GDPR y nuestra LPDP.

En el contexto de este trabajo, cabe destacar la reestructuración y actualización de los controles dando origen a la nueva versión de la Guía de Buenas Prácticas ISO 27002:2022. Esta nueva versión que agrupa los controles en: Personas, Organización, Tecnológicos y Físicos; y asocia atributos a cada control. Entre estos atributos se pueden mencionar tipos de control: preventivos, detectivos y correctivos; requisitos de la información: Confidencialidad, Integridad y Disponibilidad; Conceptos de Ciberseguridad: Identificar, Proteger, Detectar, Responder y Recuperar. Además de los conceptos de Ciberseguridad propuestos por NIST (National Institute of Standards and Technology) se incorporan controles alineados con el estado actual del arte de la seguridad informática específicamente. Entre los nuevos controles de la ISO27002:2022 se vincula con este trabajo el control **A.8.12 Data Leakage Prevention**.

6.2. Nuevo control ISO27002:2022: Data Leakage Prevention

Este control requiere que se apliquen medidas de Data Leakage para evitar la divulgación no autorizada de infor-

AJEA - Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1146.2022

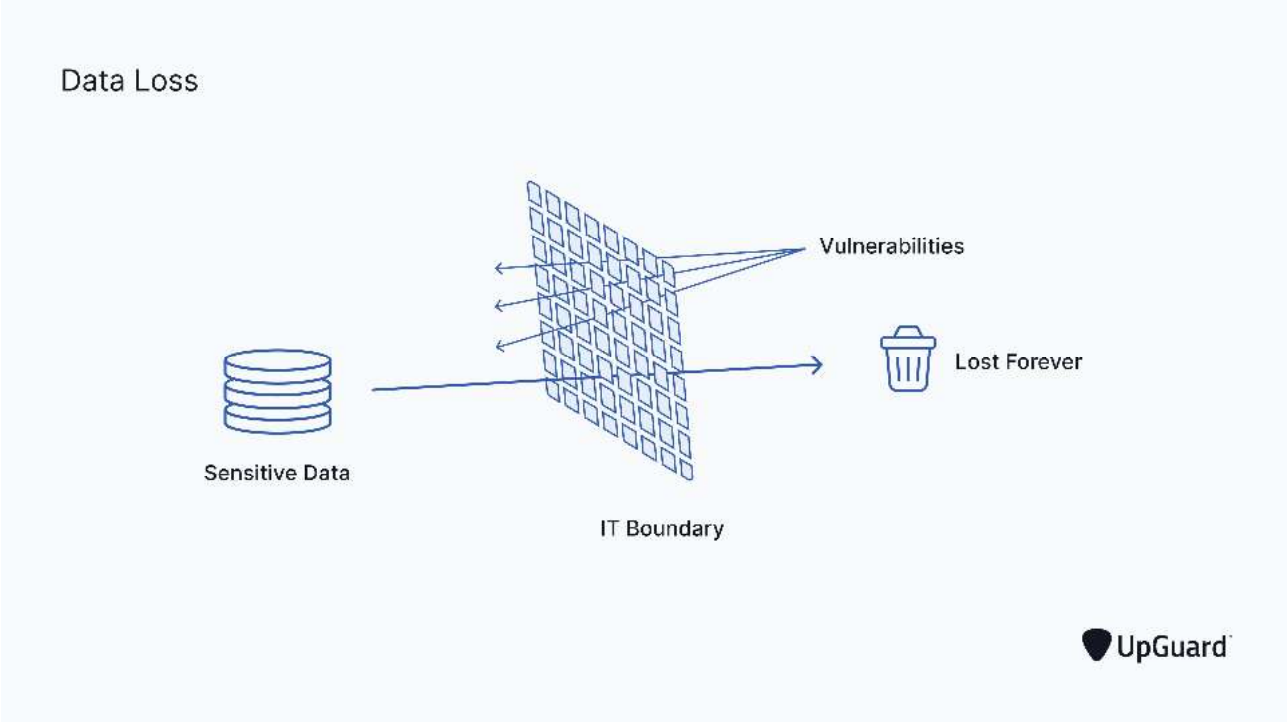

Figura 3. Data Loss

mación confidencial y, si ocurren tales incidentes, para detectarlos de manera oportuna. Esto incluye información en sistemas de TI, redes o cualquier dispositivo.

Para este propósito, se pueden utilizar sistemas para monitorear posibles canales de fuga, incluidos correos electrónicos, dispositivos de almacenamiento extraíbles, dispositivos móviles, etc, y sistemas que eviten que se filtre información, por ejemplo, deshabilitar la descarga a almacenamiento extraíble, poner en cuarentena el correo electrónico, restringir copiar y pegar datos, restringir la carga de datos a sistemas externos, cifrado, etc.

La organización debe configurar procesos que determinen la confidencialidad de los datos, evaluar los riesgos de varias tecnologías (por ejemplo, los riesgos de tomar fotos de información confidencial con un teléfono inteligente), monitorear los canales con el potencial de fuga de datos y definir qué tecnología usar para bloquear la exposición de datos sensibles.

Además, se requiere que la organización concientice a los empleados sobre qué tipo de datos confidenciales se manejan en la empresa y por qué es importante evitar fugas, capacitándolos sobre qué está permitido y qué no, cuando se manejan datos confidenciales.

En cuanto a la documentación la Guía de Buenas prácticas no hace mención, sin embargo dentro del SGSI que propone ISO 27001 se cuenta con un manual de Políticas de Seguridad de la Información que posibilita la inclusión de reglas sobre prevención de fuga de datos y que pueden asociarse a:

- Procedimientos operativos de seguridad: qué sistemas de monitoreo y prevención deben usar los administradores
- Política de uso aceptable: qué está y qué no está permitido para los usuarios habituales

6.3. Controles ISO27002 para Data Loss Prevention

Dentro de los Controles que la Guía de Buenas Prácticas propone, alguno de ellos pueden vincularse a estrategias de Data Loss Prevention:

- A.9.2.1 Registro y Cancelación del registro de usuarios.
- A.9.4.2 Procedimiento de Ingreso Seguro.
- A.9.4.3 Sistemas de Gestión de Contraseñas.
- A.10.1.1 Política sobre el uso de controles criptográficos.

AJEA - Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1146.2022

- A.11.2.7 Disposición segura o reutilización de equipos.
- A.11.2.8 Equipos de usuario desetendido.
- A.12.2.1 Controles contra códigos maliciosos.
- A.12.4.1 Registro de Eventos.
- A.12.5.1 Instalación de Software en Sistemas Operativos.
- A.13.2.1 Políticas y Procedimientos de transferencia de información.
- A.13.2.3 Mensajería Electrónica.
- A.16.1.2 Reporte de eventos de seguridad de la información.
- A.16.1.7 Recolección de Evidencia.

7. Uber sufrió un ataque informático debido a un Data Breach

El atacante, utilizó técnicas de Ingeniería Social suplantando su identidad por un empleado del área de sistemas para persuadir a un empleado y logrando el acceso a su VPN y luego escanearon la Intranet.

Una red compartida contenía scripts de powershell y uno de estos scripts contenía las credenciales de acceso para un usuario con permisos de administrador de una solución llamada PAM de thycotic que es utilizada para la gestión de accesos privilegiados. Y desde aquí accedieron al resto de los servicios.

El atacante, envió capturas para demostrar que habría logrado acceso completo a una parte importante y crítica de la infraestructura tecnológica de Uber, como son: acceso a cuentas de administrador, a los servidores de Amazon Web Service, el panel de HackerOne con el reporte de las vulnerabilidades, el canal de Slack, acceso a cuentas de administrador de vSphere y de Google Suite.

La compañía asumió la responsabilidad de haber sufrido un ataque informático y continuó operando con normalidad, pero no es posible exponer sus planes de contingencia puesto que no los han dado a conocer.

De todos modos, Uber no se puede desligar de las consecuencias legales y monetarias por esos datos accedidos por el atacante.

El caso citado es un claro ejemplo de la materialización de un riesgo asociado directamente al factor humano.

La materialización de este riesgo permite al atacante obtener información privada y sensible y generar pérdida de información, no obstante los mecanismos de Data Loss Prevention previenen que estos datos sean extendidos fuera de la red de la organización y, en caso de que el atacante quiera ejecutar esta acción, permite la detección del mismo.

8. Conclusión

Analizando los conceptos que se expusieron a lo largo de este trabajo, sumados a un ejemplo donde muchos de estos conceptos son utilizados, como la ingeniería social por parte de un atacante, la negligencia de los recursos humanos que forman parte de la organización, Data Leakage, Data Breach, Data Loss y mecanismos de Data Leak Prevention, Data Loss Prevention y Zero Trust, podemos concluir en que la seguridad de las organizaciones debe tener como eje a las personas, porque las mismas forman parte tanto del problema como de la solución. No sólo apoyándose en tecnologías que sigan las reglamentaciones de GDPR, la Ley 25.326 y las buenas prácticas de normas internacionales como las presentes en la ISO 27002 sino también en la capacitación constante de los recursos humanos.

9. Reconocimientos y agradecimientos

El presente trabajo fue realizado en el contexto del proyecto: TOECRO0008583 - ”Modelización de un Sistema de Diagnóstico de Riesgos de Seguridad de la Información para su Integración a Sistemas de Gestión de Calidad”de la Universidad Tecnológica Nacional radicado en la Facultad Regional Rosario.

Agradezco a mis perros por brindarme la mejor compañía, a mis seres queridos por escucharme hablando por horas de mi pasión que es esta carrera y a mis colegas por el apoyo y guía profesional.

Referencias

[1] Z. M. King, D. S. Henshel, L. Flora, M. G. Cains, B. Hoffman, y C. Sample, “Characterizing and measuring maliciousness for cybersecurity risk assessment,” *Varun Dutt, Indian Institute of Technology Mandi, India*, 2018.

[2] “What is a data leak? stop giving cybercriminals free access.” `https://www.upguard.com/blog/data-leak`.

[3] “6 most common causes of data leaks in 2022.” `https://www.upguard.com/blog/common-data-leak-causes`.

[4] “How much does a data breach cost in 2022?.” `https://www.ibm.com/security/data-breach`.

[5] “Iso 27001:2022.” `https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/`.

[6] R. Tahboub y Y. Saleh, “Data leakage/loss prevention systems (dlp),” 2014.

AJEA - Actas de Jornadas y Eventos Académicos de UTN
DOI: https://doi.org/10.33414/ajea.1146.2022

[7] "How the iso/iec 27001 framework supports gdpr compliance." https://gemserv.com, 2019.

[8] "Uber investigating breach of its computer systems." https://www.nytimes.com/2022/09/15/technology/uber-hacking-breach.html.