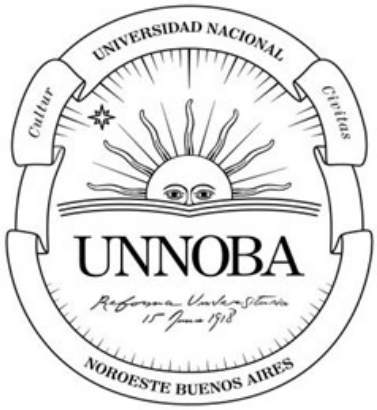

Universidad Nacional del Noroeste de la Provincia de Buenos Aires

Título:

Fortalecimiento de la ciberseguridad mediante el diseño e implementación de un Plan de Recuperación de Desastres y un Plan de Continuidad de Negocio en empresa del sector agrícola.

Carrera: Licenciatura en Sistemas

Práctica Profesional Supervisada

Estudiante: Germán Fondato

Tutor Docente: Marcelo Emanuel Guiguet

Tutor de la Empresa: Adriano Novachaelley

Fecha de Presentación: 09 de Diciembre de 2025

Índice

Tabla de Contenidos

1- Introducción

En la actualidad, las empresas dependen cada vez más de las infraestructuras tecnológicas y sistemas de información para poder llevar a cabo el desarrollo de sus procesos productivos, logísticos y administrativos. Si bien las nuevas tecnologías han optimizado notablemente la eficiencia operativa y la toma de decisiones, en consecuencia, se ha incrementado la exposición a riesgos vinculados a la ciberseguridad. Sufrir un ciberataque puede desencadenar en la interrupción de la producción, comprometer cierta información sensible o hasta incluso, generar pérdidas económicas de gran impacto [1].

Limagrain Argentina Semillas SA es una empresa agrícola dedicada a la investigación, producción y comercialización de semillas (soja, maíz, trigo y girasol), la cual junto con otras compañías ubicadas en distintas partes del mundo forman el Grupo Limagrain.

El presente informe tiene como objetivo describir el trabajo realizado en dos proyectos relacionados al área IT, más precisamente a la ciberseguridad, dentro de la empresa Limagrain Argentina Semillas SA. Uno de estos proyectos es el plan de recuperación de desastres (DRP por sus siglas en inglés) y, el segundo, es el plan de continuidad de negocio (BCP por sus siglas en inglés). Para su desarrollo, se analizaron principios de gestión de riesgos y prácticas en seguridad de la información. Además, se propusieron estrategias organizacionales y técnicas que fortalecen la resiliencia completa de la empresa, garantizando así la continuidad de sus operaciones críticas y la protección de sus activos digitales.

Ambos proyectos fueron implementados a nivel global dentro del Grupo Limagrain. En este trabajo se mostrará lo realizado en Limagrain Argentina Semillas SA, respetando la confidencialidad solicitada por la empresa.

2- Objetivos

Por un lado, se debe diseñar e implementar un DRP, definiendo políticas, procedimientos y responsabilidades necesarias para restaurar los sistemas y servicios afectados por un ciberataque, garantizando el retorno a la operatividad normal en el menor tiempo y con el menor impacto posible.

Por otro lado, el alcance y las consecuencias reales de un incidente solo pueden conocerse una vez ocurrido el mismo. Entonces, se debe desarrollar un BCP, cuyo objetivo principal es garantizar que continúen las operaciones esenciales mientras la empresa se recupera del impacto sufrido.

2.1- Objetivos Específicos

Para cumplir con el objetivo general, se establecen los siguientes objetivos específicos:

- Analizar los riesgos asociados a la infraestructura tecnológica y los sistemas de información.
- Identificar activos críticos e información vulnerable.
- Evaluar el impacto potencial de incidentes que puedan interrumpir los distintos procesos.
- Elaborar un DRP que contemple los procedimientos técnicos necesarios para restaurar los sistemas y servicios afectados.
- Elaborar un BCP para que establezca las acciones organizacionales y de gestión necesarias para mantener la operatividad crítica durante el incidente y después del incidente.
- Implementar mecanismos que garanticen la eficacia y actualización continua de ambos planes.

3- Plan de Trabajo y Carga Horaria

N°	ACTIVIDADES	TIEMPO DE DURACIÓN SEMANAS																						
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	Analisis de situación de inicio	*	*	*	*																			
2	Detectar información crítica					*	*	*	*	*														
3	Detectar aplicaciones importantes						*	*	*	*	*													
4	Configurar copias de seguridad de información										*	*	*	*										
5	Configurar copias de seguridad de aplicaciones											*	*	*	*									
6	Compra y configuración de notebooks									*	*	*	*											
7	Compra y configuración de servidor NAS													*	*	*								
8	Gestion de licencias de sistema de gestión																*	*	*					
9	Preparación de ambiente para validación de backups																*	*	*	*				
10	Prueba																				*	*	*	*	*

4- Descripción de la Práctica Profesional

4.1- Estado del Arte

Las organizaciones dependen cada vez más de las infraestructuras tecnológicas y los sistemas de información para poder llevar adelante los procesos en sus diferentes áreas de trabajo. Esta creciente dependencia conlleva un aumento en los riesgos vinculados a ciberataques. Estudios recientes evidencian un aumento significativo en los ataques cibernéticos en empresas similares a la descripta en el apartado 1, afectando tanto a la infraestructura tecnológica como a los sistemas de control [2].

Dado al aumento de riesgos, la implementación de un DRP y un BCP se ha consolidado como una práctica fundamental para mitigar los impactos que pueden generar los incidentes de ciberseguridad. Cuando ambos planes se integran de manera efectiva, permiten a las empresas no solo restaurar sus sistemas e información crítica, sino también mantener sus funciones esenciales operativas durante el evento adverso [3].

Existen marcos normativos internacionales, como son las normas ISO/IEC 27031 [4], ISO 22301 [5] y NIST SP 800-34 [6], que establecen lineamientos y buenas prácticas para la gestión de la continuidad operativa y la recuperación de sistemas de información. Sin embargo, en el ámbito agroindustrial estos marcos enfrentan desafíos particulares debido a la diversidad tecnológica y la coexistencia de dos entornos [7]:

- **Tecnologías de Información (IT)**, orientadas a la gestión de datos, comunicación y procesos de negocio (software y redes).

- **Tecnologías Operativas (OT)**, enfocadas en el control y monitoreo de procesos físicos y maquinaria en tiempo real, como producción, automatización y sistemas de energía.

En conclusión, el estado actual del conocimiento destaca que es de notoria importancia contar con estrategias integrales que combinen recuperación de información y aplicaciones con continuidad de negocio, en sectores críticos como el agropecuario, donde la interrupción de alguno de sus procesos en ciertas épocas del año puede generar daños económicos de gran relevancia [8].

4.2- Situación de inicio

Como primera medida, en Argentina (al igual que en otras regiones) se tuvo que analizar cómo se encontraba la empresa respecto tanto a respaldos de archivos como de aplicaciones y sus bases de datos, y a partir de ahí comenzar a planificar la implementación del DRP y BCP.

Si bien ambos planes no estaban implementados aún, existía una política de copias de seguridad en caso de que algo inesperado ocurriera, sea un ataque cibernético o simplemente necesitar recuperar un archivo en una fecha determinada.

Existía un servidor virtual creado específicamente para backups, en el cual a través de la aplicación Veeam Backup and Replication [9] se almacenaban copias de seguridad diarias incrementales del servidor de archivos compartidos, manteniendo siempre, como mínimo, las últimas dos. Lo mismo ocurría para la aplicación de gestión y los sistemas utilizados en los departamentos de Laboratorio y Producción, donde se realizaba una copia de seguridad a diario, en horario nocturno, de la base de datos e información de las aplicaciones manteniendo siempre como mínimo las últimas dos copias.

Sumado a lo descripto en el párrafo anterior, se realizaban copias de seguridad cruzada, es decir que lo que se almacenaba en el servidor específico para estos backups, se replicaba semanalmente en un servidor ubicado en Curitiba (y viceversa), manteniendo siempre las dos últimas copias.

4.3- Implementación del DRP

Teniendo en cuenta la situación de inicio explicada en el apartado 4.2, se tenía un panorama de qué información había que respaldar, como también de los diferentes sistemas, sea de gestión, laboratorio, producción.

Al comenzar con la implementación del plan de recuperación de desastres, se tuvo que formular una estrategia para las copias de seguridad acorde a la criticidad de los distintos sistemas e información de la empresa. La estrategia definida se explica en el apartado siguiente.

4.3.1- Estrategia de copias de seguridad

Las copias de seguridad se configuraron con el fin de garantizar la capacidad de recuperar los datos y sistemas necesarios para ser usados luego de una manipulación o eliminación accidental o maliciosa. Por lo tanto, están lo suficientemente protegidas para asegurar su resguardo en términos de confidencialidad, integridad y disponibilidad, de acuerdo con la criticidad de las actividades que respaldan.

La estrategia completa de copias de seguridad sigue el principio "**3-2-1+0**", el cual requiere de, por lo menos:

- Se deben mantener permanentemente **3** copias de los datos: la copia principal más 2 copias adicionales.
- En **2** medios y sistemas diferentes, cubriendo así el riesgo de fallas mecánicas o lógicas del sistema. Nota: una solución de replicación basada en RAID no cuenta como dos medios separados, ya que comparten una misma base de hardware.
- **1** copia fuera del sitio (offsite), ubicada en una localización externa dentro de una zona de desastre diferente, para cubrir el riesgo de caída del centro de datos o incidentes geográficos como fallas en el suministro eléctrico, desastres naturales, etc. Debe estar offline, en el sentido de estar físicamente desconectada y/o ser inalterable, para cubrir el riesgo de manipulación maliciosa o eliminación de datos, como ocurre en ataques basados en ransomware [10].
- Con **0** errores, mediante la implementación de procesos que garanticen la integridad y la usabilidad de las copias de respaldo.

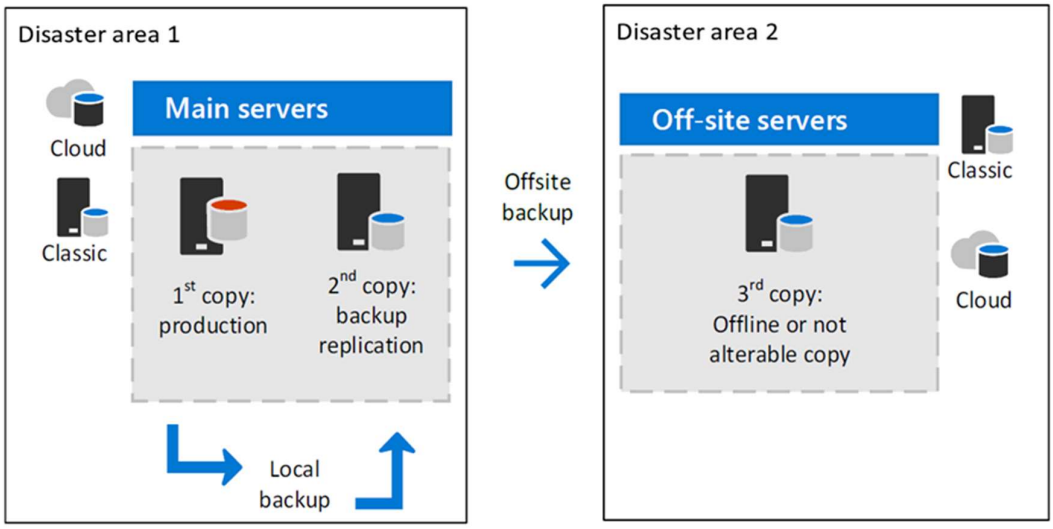

Imagen 1: Estrategia de copias de seguridad

Además, el método (sea incremental o completo), la frecuencia y los parámetros de retención se adaptaron a los objetivos de tiempo de recuperación (RTO por sus siglas en inglés) y objetivo de punto de recuperación (RPO por sus siglas en inglés) del negocio, para garantizar su usabilidad en operaciones empresariales con restricciones de tiempo [11]. Sin embargo, esta estrategia define parámetros basados en la criticidad de la solución para garantizar un nivel mínimo de protección tanto para los datos como para la configuración de los sistemas.

4.3.1.1 Backup de Sistemas

El respaldo de sistemas incluye todos los datos necesarios para reconstruir una aplicación junto con todos los componentes técnicos de soporte. Puede tratarse, por ejemplo, de respaldos completos de máquinas virtuales o simplemente de los medios necesarios para desplegar los sistemas desde cero. Se aclara además que, en los casos donde se realiza más de una copia de seguridad diaria o semanalmente, estas se hacen en diferentes momentos.

La frecuencia de respaldo y la tasa de retención de un sistema se adaptan a su criticidad:

1. Sistemas sistémicos, aquellos que en caso de sufrir inconvenientes afectan a toda la organización, con al menos:
    - 2 copias actualizadas a diario, manteniendo las últimas 14 copias, correspondientes a los últimos 7 días.
    - 1 copia offline/offsite o no alterable actualizada semanalmente, manteniendo las últimas 6 copias.
    - 1 copia mensual, manteniendo las últimas 2 copias.

- 0 errores con comprobaciones diarias.

2. Sistemas críticos, son los que de sufrir inconvenientes afectan a una región, país o parte de la empresa, con al menos:
    - 2 copias actualizadas a diario, manteniendo las últimas 14 copias, correspondientes a los últimos 7 días.
    - 1 copia offline/offsite o no alterable actualizada semanalmente, manteniendo las últimas 4 copias.
    - 1 copia actualizada mensualmente, manteniendo solo 1 copia.
    - 0 errores con comprobaciones diarias.
3. Sistema moderado, con al menos:
    - 2 copias actualizadas a diario, manteniendo las últimas 3 copias.
    - 0 errores con comprobaciones semanales.
4. Sistema bajo, con al menos:
    - 2 copias actualizadas semanalmente, manteniendo las últimas 3 copias.
    - 0 errores con comprobaciones semanales.

Al aplicar la estrategia en Argentina, se tuvieron en cuenta tres aplicaciones. Una de ellas, Softland ERP (Planificador de Recursos Empresariales por sus siglas en inglés), es el sistema de gestión utilizado por todas las áreas de la empresa. Las otras dos, llamadas Labo y Pron, son utilizadas por las áreas de Laboratorio y Producción respectivamente, almacenando toda la información de dichos departamentos. De acuerdo con la criticidad de los datos, se clasifican como sistemas críticos.

4.3.1.2 Backup de datos

El respaldo de datos incluye la información de negocio utilizada dentro del sistema, como el contenido del data lake, bases de datos NoSQL, archivos, etc. En cuanto a los casos donde se realiza más de una copia de seguridad diaria o semanal, se maneja de la misma manera especificada en el punto 4.3.1.1.

La frecuencia de respaldo y la tasa de retención de los datos se adapta a su criticidad:

1. Dato sistémico, con al menos:
    - 2 copias actualizadas a diario, manteniendo las últimas 14 copias, correspondientes a los últimos 7 días.
    - 1 copia offline/offsite o no alterable actualizada semanalmente, manteniendo las últimas 10 copias, correspondientes a las últimas 10 semanas.
    - 1 copia actualizada mensualmente, manteniendo las últimas 6 copias.
    - 0 errores con comprobaciones diarias.
2. Dato crítico, con al menos:

- 2 copias diariamente actualizadas, manteniendo las últimas 14 copias, correspondientes a los últimos 7 días.
- 1 copia offline/offsite o no alterable actualizada semanalmente, manteniendo las últimas 7 copias.
- 1 copia actualizada mensualmente, manteniendo las últimas 3 copias.
- 0 errores con comprobaciones diarias.

3. Dato moderado, con al menos:
    - 2 copias actualizadas a diario, manteniendo las últimas 7 copias.
    - 0 errores con comprobaciones semanales.
4. Dato bajo, con al menos:
    - 2 copias actualizadas semanalmente, manteniendo las últimas 3 copias.
    - 0 errores con comprobaciones semanales.

En Argentina, se aplicó la estrategia de copia de seguridad de datos en dos servidores de archivos compartidos. Uno cuenta con una carpeta para cada departamento de la empresa y los usuarios trabajan a diario en él. El restante, solo es utilizado por las áreas de Mantenimiento, Producción, Laboratorio y Logística, también a diario. Debido a la sensibilidad de los datos, se clasifican como críticos.

4.3.1.3 Prueba de recuperación de backup

La recuperación de la copia de seguridad se prueba de acuerdo con la criticidad del sistema o de los datos.

Los backups de los sistemas calificados como sistémicos deben ser probados al menos cada 5 años hasta el nivel aplicativo, lo que implica realizar una restauración completa de los componentes técnicos (máquinas virtuales, servidores, etc.), la aplicación y los datos asociados, y ejecutar pruebas de aceptación de usuario sobre ellos.

Por su parte, el respaldo de los sistemas calificados como críticos deben ser probados al menos cada 5 años, de forma idéntica a los sistémicos, pero sin realizar pruebas de aceptación de usuario.

Por último, la frecuencia de prueba de los sistemas calificados como moderados y bajos queda a criterio del área de negocio, del equipo de soporte del sistema y de los equipos técnicos.

4.3.1.4 Seguridad de los backups

Los sistemas de copias de seguridad están aislados de otros entornos, es decir, los sistemas de respaldo deben estar segregados de la red de producción y de sus componentes (Active Directory, máquinas anfitrionas, hipervisores, etc.) para prevenir manipulaciones maliciosas del sistema y/o de los datos.

Además, los sistemas de respaldo y su ejecución están supervisados y garantizan la integridad y confidencialidad de los datos. Para implementar la propiedad de error cero de la estrategia, debe aplicarse el siguiente proceso:

- Se supervisa la adecuada ejecución de los respaldos para garantizar que se realicen con la periodicidad correspondiente y se completen con éxito, especialmente en los sistemas críticos y sistémicos.
- Se implementan pruebas que aseguran la integridad de las tareas de respaldo y de los datos respaldados, mediante el uso de mecanismos criptográficos basados en funciones hash [12] y firmas digitales [13].
- Toda alerta o desviación es debidamente atendida y gestionada.

Los datos respaldados son replicados y distribuidos con el objetivo de asegurar su conservación, aunque esto también incrementa su nivel de exposición. Por esta razón, la protección de la confidencialidad, por ejemplo, mediante el uso de mecanismos de cifrado, es obligatoria tanto para los datos en reposo como en tránsito. La clave de cifrado asociada debe mantenerse bajo los mismos estándares de confidencialidad, integridad y disponibilidad que los datos que protege.

Es imprescindible asegurar la inmutabilidad de los respaldos offline para protegerlos contra manipulaciones accidentales o ataques maliciosos a largo plazo.

Los datos respaldados son monitoreados para detectar cambios sospechosos. Se implementa la detección de estos mediante mecanismos de análisis estructural, estadístico y de inteligencia artificial, con el fin de identificar ataques dirigidos contra los datos respaldados a nivel de aplicación.

4.3.2- Compra y configuración de equipos

4.3.2.1- Laptops

Para la implementación de los proyectos en Argentina, se definió que se debía comprar 5 laptops y para cada una de ellas una garantía específica de 4 años. Las mismas debían contar con las siguientes características:

- Marca HP, línea Probook 445 G9.
- Procesador: AMD R5-5600.
- Memoria RAM: 16GB.
- Disco de estado sólido: 256GB.
- Garantía de 4 años en sitio al siguiente día laboral.

Imagen 2: Laptop HP Probook 445 G8

Se solicitó cotización a tres proveedores diferentes y una vez se recibieron las mismas se avanzó con la compra de la más conveniente teniendo en cuenta relación de precio y tiempo de entrega. Por confidencialidad, se omiten valores de compra, nombre de proveedores y demás información que pueda comprometer a la empresa.

Una vez se recibieron los equipos, se configuraron de la manera estándar propuesta a nivel global, como se detalla a continuación.

Primero, se configuró la versión original de Windows 10 que el laptop tenía por defecto. Durante esta configuración, se utilizaron los siguientes parámetros:

1. El nombre del equipo está basado en CN+SITECODE+DRP+SEQ donde:
    a. CN: Computer Notebook.
    b. SITECODE: Se utiliza el código del sitio para identificar a qué compañía pertenece la notebook, teniendo en cuenta que las computadoras que tenemos son para las distintas unidades de negocio.
    c. DRP: Solo para especificar que estas computadoras son específicas para el proyecto DRP.
    d. SEQ: Tres dígitos numéricos utilizados como secuencia.
    e. Ejemplos: CNAR-PRO-DRP001, CNAR-PRO-DRP002, CNAR-PRO-DRP003, CNAR-PRO-DRP004 y CNAR-PRO-DRP005.
2. Creación del usuario administrador.
3. Creación de usuario local, con permisos por defecto, sin ser administrador.
    a. Nombre de usuario: AR-DRP001 (Donde AR corresponde al país, DRP indica que pertenece al proyecto y 001 la secuencia del nombre del equipo).

Luego, se desinstalaron las aplicaciones que no iban a ser necesarias (como Spotify, Netflix, Xbox, etc).

Posteriormente, se instalaron las aplicaciones estándares del proyecto BCP.

- Microsoft Office 2021 Estándar, con código de licencia local y lenguaje español. Incluyendo las aplicaciones Access, Excel, Word, PowerPoint, OneNote, OneDrive.

- 7zip. Utilizado para descomprimir archivos de ser necesario.
- MS Edge. Navegador de internet.
- Adobe PDF Reader. Lector de PDF.
- Keepas. Gestor de contraseñas.
- Controlador de impresora local.

Finalmente, se agregaron las laptops al inventario donde se manejan todos los dispositivos de la empresa.

Los días 22 de cada mes (o lunes siguiente en caso de ser fin de semana), se encienden los cinco equipos, se verifica su funcionamiento como también el de cada una de las aplicaciones instaladas, se buscan actualizaciones disponibles y en caso de haber se instalan.

Las computadoras se configuraron sin tener conexión con la red corporativa, es decir que son completamente externas. Se realizó de esta manera, ya que, en caso de sufrir un inconveniente, puede que no se tenga acceso a, por ejemplo, Active Directory y estando dentro de la red no funcionan. De este modo, sólo se utilizarán con conexión a cualquier red y con usuarios locales.

4.3.2.2- Servidor NAS

Dado que era necesario más espacio para poder almacenar las copias de seguridad y así mantenerlas a través del tiempo, se optó por la compra de un servidor NAS QNAP.

Siguiendo la metodología aplicada para la compra de laptops explicada en la sección 4.3.2.1, del mismo modo se realizó para la compra del servidor.

Se solicitó cotización del siguiente servidor:

- NAS QNAP TS-431k, 4 BAY, 4 CORE, 1.7 GHZ, 1GB
- 3 discos duros de 12 TB cada uno.

Imagen 3: Servidor NAS QNAP TS-431k

Se solicitaron cotización a tres proveedores diferentes y una vez se recibieron las mismas se avanzó con la compra de la más conveniente teniendo en cuenta relación de precio y logística. Por confidencialidad, se omiten valores de compra, nombre de proveedores y demás información que pueda comprometer a la empresa.

Una vez recibido el equipo, se instaló en el rack de la sala de servidores, se encendió y se conectó a la red interna a través de una conexión LAN para poder realizar las configuraciones correspondientes.

Primero, se detectó el equipo dentro de la red y se le asignó una dirección IP estática y nombre de host.

Posteriormente se creó una carpeta dentro del servidor que se compartió en la red para poder almacenar las diferentes copias de seguridad.

4.4- Implementación del BCP

Un BCP consiste en un conjunto de estrategias, procedimientos y medidas diseñadas para garantizar que una organización pueda seguir operando durante y después de una interrupción grave (como puede ser un ciberataque). En otras palabras, es un plan que busca que el negocio no se detenga si ocurre algún evento que afecte su funcionamiento normal [14].

Como punto de partida para su implementación, se llevaron adelante diversas reuniones con gerentes de distintas áreas con el objetivo de determinar qué carpetas y/o archivos era necesario respaldar y con qué periodicidad cada uno de ellos.

Estos archivos son almacenados en un Sharepoint, ubicado en un servidor de Azure [15] con el fin de poder ser accesibles en caso de tener eventos que no nos permitan utilizar nuestra red interna o nuestros servidores.

Algunos de estos archivos se respaldan diariamente, otros semanalmente, y el resto de forma mensual, dicho tiempo dependerá de la frecuencia con la que cada archivo o carpeta es modificado y cada usuario que modifique el archivo deberá sincronizarlo en el Sharepoint. Los gerentes de cada área son los encargados de verificar que todos los archivos estén actualizados dentro del Sharepoint antes mencionado.

Dentro de la empresa se creó un comité de crisis integrado por gerentes de alto nivel jerárquico que, entre otras cuestiones, posee credenciales (usuario y contraseña) para acceder al Sharepoint donde se encuentran los respaldos, que en caso de activación del plan compartirán con los usuarios que corresponda para que puedan descargar los archivos necesarios. Es importante aclarar que, estas credenciales serán necesarias cuando el dominio corporativo no esté disponible.

Sumado a lo mencionado anteriormente, los usuarios poseen celulares con conexión 4G, que utilizarán como hotspot [16] en caso de que la red corporativa no esté disponible.

4.4.1- Roadmap de Ciberataque – Respuesta a Incidentes

A continuación, se muestra la estrategia en detalle de la respuesta a incidentes, la cual cuenta con cuatro fases.

Fase 1: Detección de evento

1. Plan de acción de emergencia (PAE por sus siglas en inglés).
    a. No apague los dispositivos/equipos afectados.
    b. Desconectar de la red internet los dispositivos involucrados, desconectando el cable o desactivando wifi.
    c. Una vez el dispositivo está aislado, proceder a comunicar el evento a través de las herramientas disponibles de acuerdo con el escenario.
2. Flash Alert de evento de ciberataque.
    a. Reportar el evento de acuerdo con la instrucción de la alerta.
    b. Si se estima que el evento es de categoría de crisis 2 o 3, informar inmediatamente a la compañía para organizar la gestión de crisis. Las categorías de los eventos se detallarán más adelante como escenarios de crisis.

Fase 2: Proceso de Gestión de Crisis

1. Lanzamiento del proceso de gestión de crisis.
    a. Evaluación y descripción del evento.
    b. Evaluación de crisis. Determinar/validar la evaluación del nivel de crisis.
    c. Unidad de crisis interna. Nombramiento del comité de crisis de acuerdo con la unidad de negocio.
    d. Análisis de la crisis. Determinar el escenario de la crisis para definir las acciones que se llevarán a cabo en el BCP.
    e. Partes interesadas. Determinar las partes involucradas, afectadas por la crisis.
    f. RTO. Tiempo máximo aceptable para restaurar las actividades críticas tras una interrupción no planificada.
    g. RPO. Tiempo transcurrido desde la última copia de seguridad fiable.
    h. Definición del estado final deseado (DES por sus siglas en inglés). Restablecer información, sistemas y equipos para que el equipo trabaje con normalidad.

Fase 3: Modelo degradado

1. Activación del BCP refiriendo a los escenarios del 1 al 5 de acuerdo con las tablas definidas por sitio/actividad.
    a. No detener actividades críticas (ver tabla 1).
    b. Informar al staff.
        i. Personas claves a bordo (ver tabla 2).
        ii. Resto del personal. Decisión pendiente.
    c. Distribución de las laptops configuradas para el DRP al personal crítico para cada actividad.
    d. Activar los procedimientos manuales. El personal operativo clave recibe los procedimientos escritos (ver tabla 3).
    e. Organizar al personal con los datos del respaldo más reciente.
        i. Entrega de los datos desde la copia de seguridad en archivos digitales en formato Excel o en papel (ver tabla 3).
    f. Comunicación. Emisión, autorización y control de notas informativas en el extranjero.

List Activities & Sub-activities by site

Country	Site	Activity	Sub-activity	Comments
Argentina	Pergamino - BA	HR (Payroll)	**Staff admission**	Access to Gov.Web
Argentina	Pergamino - BA	HR (Payroll)	**Staff resignation**	Access to Gov.Web
Argentina	Pergamino - BA	HR (Payroll)	**Salary Payment**	Active personnel control data
Argentina	Pergamino - BA	Sales and Customer service	**Sales order collection form**	Consider gmail-box for sales in spare NB. WhatsApp Group
Argentina	Pergamino - BA	Sales and Customer service	**Credit Analysis**	Check the customer assessment
Argentina	Pergamino - BA	Sales and Customer service	**Loading order release**	Send sales orders authorized to distribution clusters
Argentina	Pergamino - BA	Finances	**Bank Incomes & outcomes**	Web access

Tabla 1: Lista de actividades y subactividades por sitio.

List employees involved in critical activities by site

Country	Site	Activity	Sub-activity	Name	Role	Phone
Argentina	Pergamino - BA	HR (Payroll)	**All activities**		main contact	
Argentina	Pergamino - BA	HR (Payroll)	**All activities**		secondary contact	
Argentina	Pergamino - BA	Sales and Customer service	**Sales order collection form**		main contact	
Argentina	Pergamino - BA	Sales and Customer service	**Credit Analysis**		main contact	
Argentina	Pergamino - BA	Sales and Customer service	**Loading order release**		main contact	
Argentina	Pergamino - BA	Sales and Customer service	**Sales order collection form**		secondary contact	
Argentina	Pergamino - BA	Sales and Customer service	**Credit Analysis**		secondary contact	
Argentina	Pergamino - BA	Sales and Customer service	**Loading order release**		secondary contact	
Argentina	Pergamino - BA	Sales and Customer service	**Sales order collection form**		secondary contact	
Argentina	Pergamino - BA	Sales and Customer service	**Credit Analysis**		secondary contact	
Argentina	Pergamino - BA	Sales and Customer service	**Loading order release**		secondary contact	
Argentina	Pergamino - BA	Finances	**Bank Incomes & outcomes**		main contact	
Argentina	Pergamino - BA	Finances	**Bank Incomes & outcomes**		secondary contact	

Tabla 2: Lista de empleados involucrados en actividades críticas por sitio.

List of Data Extraction

Country	Site	Activity	Sub-activity	Document type	Win code	Responsible	Starting data, necessary for BCP	Database for Extraction	Digital File	Backup frequency	Paper format	Backup frequency	Emergency Folder	Folder Rights To
Argentina	Pergamino - BA	HR (Payroll)	Salary Payment	Data base extraction			Database of staff on board		Excel	Weekly	Yes	On demand		
Argentina	Pergamino - BA	Sales and Customer service	Credit Analysis	Data base extraction			Limite de creditos - Exposicion		Excel	Daily	Yes	On demand		
Argentina	Pergamino - BA	Sales and Customer service	Sales orders pending delivery	Data base extraction			Listado de pendientes de remitir		Excel	Daily	Yes	On demand		
Argentina	Pergamino - BA	Sales and Customer service	Customer master file	Data base extraction			Ficha de clientes		Excel	Daily	Yes	On demand		
Argentina	Pergamino - BA	Sales and Customer service	Commisions to be payed	Data base extraction			Listado de comisiones pendientes		Excel	Daily	Yes	On demand		
Argentina	Pergamino - BA	Sales and Customer service	Commercial conditions	Data base extraction			Listado de condiciones comerciales		Excel	On demand	Yes	On demand		
Argentina	Pergamino - BA	Sales and Customer service	Base de datos de productos	Data base extraction			maestro de productos		Excel	Yearly	Yes	On demand		
Argentina	Pergamino - BA	Sales and Customer service	Base de datos de productos	Data base extraction			Stock DISPONIBLE FCTS sobre SOFTLAND		Excel	Daily	Yes	On demand		
Argentina	Pergamino - BA	Sales and Customer service	Legal invoicing forms	Register			Formularios pre impresos facturas A y B		?	On demand	Yes	On demand		
Argentina	Pergamino - BA	Sales and Customer service	Pedido de Ventas	Register			Formulario digital e impreso de Pedido de Ventas		Excel	Yearly	Yes	On demand		
Argentina	Pergamino - BA	Sales and Customer service	Word de Walter	Procedure			Procedimiento escrito de Modo Degradado		Word	Yearly	Yes	On demand		
Argentina	Pergamino - BA	Sales and Customer service	Facturas pendientes de Cobro	Data base extraction			Softland		Excel	Daily	Yes	On demand		
Argentina	Pergamino - BA	Finance	Facturas pendientes de Pago	Data base extraction			Softland		Excel	Daily	Yes	On demand		

Tabla 3: Lista de extracción de datos.

Fase 4: Regreso a la normalidad

1. Cierre. DES alcanzado, información restaurada y normalidad en actividades.
    a. El departamento de IT informa a la empresa que se levanta el aislamiento de internet.
    b. Ponerse al día con el retraso de la trazabilidad local y datos en las aplicaciones.
    c. Verificación de la coherencia de los datos en las aplicaciones.
    d. Cuando finaliza el análisis, reanudar las actividades con normalidad y cerrar la crisis.

4.4.2- Escenarios de Crisis

Se plantearon cinco escenarios de crisis diferentes, con el objetivo de saber cómo responder ante los efectos que pueda generar un ciberataque.

Escenario 1: Indisponibilidad de computadoras de usuario. En este escenario se supone que más del 50% de las computadoras de los usuarios quedan indisponibles. Estrategia:

- Desconectar todas las computadoras de la red.
- Evaluar el número y la ubicación de los equipos afectados.
- Apagar las computadoras afectadas de ser necesario.
- Distribuir computadoras al personal crítico.
- Activar procedimientos manuales. Organizar al personal con los respaldos de información.
- Vuelta a la normalidad. Cuando el personal tiene nuevamente su equipo, debe ponerse al día con el trabajo pendiente y actualizar los datos en las aplicaciones.

Escenario 2: Indisponibilidad de aplicaciones críticas. Estrategia:

- Informar al personal sobre las aplicaciones críticas que no están disponibles debido al ataque cibernético, basado en un reporte proporcionado por el departamento de IT.
- Activar procedimientos manuales. Organizar al personal con los respaldos de información. Se recupera la información desde los respaldos tan rápido como sea posible.
- Vuelta a la normalidad. El departamento IT informa a la empresa que las aplicaciones críticas están activas nuevamente. Se debe poner al día con el trabajo pendiente, actualizar los datos en las aplicaciones y verificar la consistencia de los datos en la misma. Al finalizar el retraso, continuar las tareas con normalidad.

Escenario 3: Se pierde información de entre las últimas 24 a 72 horas. Estrategia:

- El departamento IT informa al personal sobre la pérdida de información y que frene sus actividades hasta que el comité de crisis tome una decisión.
- Verificar la información restaurada desde la copia de seguridad y ponerse al día con el trabajo atrasado.

Escenario 4: Aislamiento de la red de uno o varios sitios. Al menos uno de los sitios principales está aislado por razones de seguridad. El personal de dicho sitio no puede acceder a las aplicaciones (en línea en servidores internos al lugar). Estrategia:

- Informar al personal sobre los sitios aislados.
- Activar procedimientos manuales en las sedes centrales si están aisladas.
- Activar procedimientos manuales en áreas de producción e investigación si estas están aisladas, dado a que son las actividades más críticas.
- Suspender actividades en otros sitios si están aislados.
- Vuelta a la normalidad. Se informa que los sitios afectados se encuentran nuevamente conectados a la red. Se debe poner al día con el trabajo pendiente, actualizar los datos en las aplicaciones y verificar la consistencia de los datos en la misma. Al finalizar el retraso, continuar las tareas con normalidad.

Escenario 5: Aislamiento global de internet. Todas las unidades de negocio de la empresa están completamente aisladas de internet por razones de seguridad. El personal no puede acceder a aplicaciones en línea ni sitios web. Estrategia:

- Informar al personal sobre el aislamiento global de internet.
- Activar procedimientos manuales en las sedes centrales. Las actividades más críticas para mantener son la gestión de crisis, recursos humanos, investigación, producción, finanzas y servicio al cliente. Se deberán conectar a la red utilizando sus celulares como anclaje de internet a través de la conexión 4G, sin posibilidad de acceso a la red VPN.

- Suspender actividades en otros sitios. Se informará una vez el problema haya sido resuelto.
- Finalmente, una vez solucionado se informa que todos los sitios se encuentran nuevamente conectados a la red. Se debe poner al día con el trabajo pendiente, actualizar los datos en las aplicaciones y verificar la consistencia de los datos en la misma. Al finalizar el retraso, continuar las tareas con normalidad.

4.5 Prueba de activación del DRP

Para comenzar, es indispensable aclarar que para llevar adelante esta prueba se coordinó una fecha específica con los usuarios y gerentes correspondientes de acuerdo con su disponibilidad. Además, esta simulación no se pudo realizar en su totalidad como se haría en un caso real debido a que los respaldos, tanto del sistema de gestión (aplicación Softland) como de los archivos, no se restauraron en las bases de producción, ya que la compañía continuaba con sus operaciones diarias normalmente.

Como se mencionó en el párrafo anterior, al no poder aplicar los respaldos en los servidores y bases de producción reales, fue necesario preparar el ambiente de trabajo. El mismo se realizó sobre tres de las laptops compradas y configuradas durante la etapa de implementación del DRP.

Por un lado, se debió poner en funcionamiento la aplicación Softland, lo que incluyó dos etapas:

1. Gestionar la compra de una licencia de aplicación.
2. Creación de usuarios y asignación de accesos dentro de la aplicación.

Dado a que solo se utilizará la aplicación al momento de realizar las pruebas, se optó por comprar una licencia temporal con duración de tres meses, por lo que se solicitó a la empresa Softland una cotización de esta. Luego de recibida la cotización y realizadas las aprobaciones correspondientes, se avanzó con la compra. Posteriormente, se instaló la aplicación Softland en las laptops y se activó con la licencia adquirida.

Con el sistema de gestión ya instalado y activado, se crearon manualmente los usuarios que realizan las pruebas y se copió para cada uno de ellos los accesos que le corresponden. Dichos usuarios fueron definidos anteriormente por los gerentes de las áreas involucradas: producción, finanzas y ventas.

Por otro lado, se realizó la descarga de un respaldo de la información y de la base de datos de Softland dos días antes de la fecha definida para realizar la simulación. Al

día siguiente, se copiaron ambos respaldos en las tres laptops, dejando así la aplicación y los archivos listos para las pruebas.

Ulteriormente, llegado el día del simulacro se reunió a los usuarios involucrados de cada área en una sala de reuniones. Por cada área se entregó una laptop, y se comunicó la fecha del respaldo para que tuvieran en cuenta que lo que se trabajó posteriormente no estaría. Cada persona se encargó de verificar el funcionamiento de sus tareas críticas dentro de la aplicación y de encontrar los archivos necesarios para realizar su trabajo diario.

De cada una de las pruebas se hicieron registros, si bien los datos utilizados en las tareas de altas y cargas son ficticios, se omiten incluir porque pueden contener información confidencial.

Finalmente, el resultado de la simulación fue positivo. Los involucrados no encontraron errores en el funcionamiento del sistema de gestión, como en la recuperación de archivos.

Particularmente, respecto a las aplicaciones Labo y Pron, no se realizaron pruebas al momento.

4.6 Prueba de activación del BCP

Una vez implementado el BCP, se realizaron diversas pruebas para verificar su correcto funcionamiento y ajustar posibles fallas detectadas durante el proceso. Estas pruebas se llevaron a cabo en las áreas de Producción, Laboratorio, Finanzas y Ventas.

Para llevar adelante estas simulaciones, primero se reunió en una sala de reunión a cada gerente y algunos usuarios de los departamentos correspondientes, donde se les informó que a partir de ese momento sus computadoras, la red y los servidores quedaban inaccesibles, aunque las tareas que realizarán no tendrían impacto sobre los servidores y sistemas operativos, ya que era un simulacro.

Se les otorgaron cuatro de las computadoras configuradas en la etapa de implementación del DRP, con las credenciales pertinentes, para que puedan llevar adelante las operaciones que ellos crean necesarias probar.

Como primer paso, utilizaron sus celulares con red 4G como hotspot para conectarse a wifi [17], luego el comité de crisis les otorgó las credenciales para que puedan acceder al Sharepoint donde se encuentran los backups y descargar todo lo necesario de allí. Finalmente, realizaron las tareas operativas donde se pidió a los usuarios tomar registros de los resultados que obtenían.

El resultado de la prueba fue positivo, ya que no se registraron inconvenientes. Los usuarios pudieron acceder a la información necesaria y realizar las operaciones críticas de cada proceso de manera correcta.

4.7 Trabajo Futuro

Si bien, luego de muchas horas de trabajo y gestión, se lograron implementar ambos proyectos en su totalidad en Argentina, es necesario continuar con sus tareas recurrentes para el futuro:

- Supervisar la realización de backups diarios, semanales, o mensuales de acuerdo con su correspondencia, en relación con el proyecto DRP.
- Mantener la conectividad con el Sharepoint donde se almacenan los respaldos del proyecto BCP.
- Por parte de los usuarios, continuar con la carga de los archivos en el Sharepoint del BCP para mantenerlos actualizados.
- Verificar el funcionamiento de las cinco computadoras destinadas al proyecto DRP.
- Continuar simulando la activación de ambos proyectos para verificar si todo continúa funcionando de manera correcta, al menos cada 5 años.
- Mantener la documentación de ambos proyectos actualizada. Por ejemplo, se puede dar el caso que alguna persona involucrada en cierta tarea deje la compañía, entonces se debe actualizar quien asumirá su rol.
- Mejora continua. Es necesario mantenerse alerta sobre la aparición de nuevos avances o nuevas tecnologías que ayuden a mejorar los procedimientos.

5- Conclusiones

La implementación de un DRP y un BCP constituye un pilar fundamental para garantizar la resiliencia operativa en cualquier organización en un entorno donde los riesgos operativos y tecnológicos son cada vez más frecuentes y disruptivos. A lo largo de este trabajo se evidenció que la continuidad del negocio no debe entenderse únicamente como la respuesta reactiva a incidentes, sino como una estrategia integral que permita anticipar, mitigar y gestionar eventos que puedan comprometer la disponibilidad de los servicios críticos.

El análisis desarrollado demuestra que ambos planes bien diseñados e implementados no solo reducen el impacto económico y operativo de un incidente, sino que también favorecen la capacidad adaptativa de la empresa, mejoran su postura de ciberseguridad y respaldan el cumplimiento normativo. Asimismo, se destacó la importancia de realizar evaluaciones periódicas junto con pruebas regulares de los procedimientos definidos, ya que estos procesos permiten ajustar los planes en función de cambios tecnológicos, estructurales o de contexto.

Como se ha mostrado a lo largo del presente informe, fue posible abordar y alcanzar el objetivo general propuesto, consistente en el diseño e implementación del DRP y del BCP, luego de analizar los riesgos asociados a la infraestructura tecnológica y los sistemas de información, e identificar los activos críticos y la información vulnerable.

En síntesis, la continuidad del negocio debe considerarse como un proceso evolutivo y dinámico, que requiere del compromiso organizacional, actualización continua y una cultura involucrada a la prevención. Las organizaciones que adoptan un enfoque proactivo en materia de DRP y BCP no solo aseguran la preservación de sus operaciones ante eventos adversos, sino que además adquieren una ventaja estratégica, posicionándose como entidades confiables, sostenibles, y preparadas para afrontar los desafíos del entorno actual.

6- Bibliografía

[1] A. Kulkarni, Y. Wang, M. Gopinath, D. Sobien, A. Rahman, F. A. Batarseh, “A Review of Cybersecurity Incidents in the Food and Agriculture Sector,” arXiv preprint arXiv:2403.08036, Mar. 2024.

[2] Food and Ag-ISAC, “Cyber attacks on food and agriculture sector surge 27% in 2024, report reveals,” Food Ingredients First, 2024. [En Linea]. Disponible en: https://www.foodingredientsfirst.com/news/cyber-attacks-food-agri-ransomware-food-and-ag-isac.html. 05 de Noviembre de 2025.

[3] M. Sharma and S. Bhatia, “Integrating business continuity and disaster recovery planning in critical infrastructure sectors,” Journal of Information Security and Applications, vol. 75, p. 103550, 2023.

[4] International Organization for Standardization, ISO/IEC 27031:2011 – Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity, ISO, Geneva, Switzerland, 2011.

[5] International Organization for Standardization, ISO 22301:2019 – Security and resilience – Business continuity management systems – Requirements, ISO, Geneva, Switzerland, 2019.

[6] National Institute of Standards and Technology (NIST), Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems, U.S. Department of Commerce, Gaithersburg, MD, 2010.

[7] Food and Agriculture Organization of the United Nations (FAO), Cybersecurity in the agri-food sector: Risks, challenges and strategies for resilience, Rome, Italy, 2023.

[8] CyberSecurity News, “El sector agroalimentario valenciano pierde 100 millones al año por ciberataques,”[En Línea]. Disponible en : https://cybersecuritynews.es/el-sector-agroalimentario-valenciano-pierde-100-millones-al-ano-por-ciberataques/. [Accedido: 06 de Julio de 2025].

[9] Veeam® Software “Veeam” [En línea]. Disponible en: https://www.veeam.com/. [Accedido: 30 de octubre de 2025].

[10] S. Vehabovic, N. Ghani, E. Bou-Harb, J. Crichigno y A. Yayimli, “Ransomware Detection and Classification Strategies”, 2022 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), pp. 316-324, Jun. 2022.

[11] E. K. Smith, “Business continuity management and disaster recovery: Understanding RTO and RPO,” Journal of Business Continuity & Emergency Planning, vol. 12, no. 3, pp. 234–243, 2019.

[12] National Institute of Standards and Technology, FIPS PUB 202: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, Aug. 2015.

[13] National Institute of Standards and Technology, FIPS PUB 186-4: Digital Signature Standard (DSS), 2024 (revisión final / cobertura DSA, RSA, ECDSA).

[14] R. L. Kliem and G. D. Richie, Business Continuity Planning: A Project Management Approach. Boca Raton, FL, USA: CRC Press, 2015.

[15] Microsoft, “SharePoint Server in Microsoft Azure,” Microsoft Docs, 20 Ene. 2023. [En línea]. Disponible en: https://learn.microsoft.com/en-us/sharepoint/administration/sharepoint-server-in-microsoft-azure. [Accedido: 11 de Noviembre de 2025].

[16] S. Wolfe, “Management of mobile hotspot connections”, U.S. Patent US20110294502A1, Archivo 31 de Mayo, 2010, publicado el 1 de Deciembre 2011.

[17] Rui Du, Hailiang Xie, Mengshi Hu, Narengerile, Yan Xin, Stephen McCann, Michael Montemurro, Tony Xiao Han y Jie Xu, “An Overview on IEEE 802.11bf: WLAN Sensing,” arXiv preprint, 2023.

7- Acrónimos

Acrónimo	Descripción
DRP	Plan de Recuperación de Desastres
BCP	Plan de Continuidad de Negocio
ISO	Organización Internacional de Estandarización
IEC	Comisión Electrotécnica Internacional
NIST	Instituto Nacional de Estándares y Tecnología
IT	Tecnología de la Información
OT	Tecnología Operativa
RTO	Objetivos de Tiempo de Recuperación
RPO	Objetivo de Punto de Recuperación
ERP	Planificador de Recursos Empresariales
HP	Hewlett Packard
RAM	Random Access Memory
AMD	Advanced Micro Devices
PDF	Portable Document Format
WiFi	Wireless Fidelity
NAS	Network Attached Storage
PAE	Plan de Acción de Emergencia
DES	Definición del estado final deseado
VPN	Virtual Private Network

8- Agradecimientos

Agradezco profundamente a:

- Mi familia en primer lugar, por el apoyo incondicional durante toda mi carrera universitaria y además en mis proyectos profesionales y personales.
- Mis compañeros de estudio, gracias a ellos se hizo algo más fácil.
- Mis docentes, por las enseñanzas y oportunidades ofrecidas.
- La UNNOBA por ofrecerme la posibilidad de formarme profesionalmente.