

# DIPLOMADO EN REDTEAM

## INFORME EJECUTIVO

**24 Septiembre 2021**

### INTEGRANTES:

- CRISTIAN MUÑOZ
- CRISTIAN VARGAS
- CRISTIAN VERA
- SEBASTIAN DÖLL
- SEBASTIAN HOLLOWAY

#### Acuerdo de Confidencialidad

A través del presente documento comunicamos a ustedes que toda la información, documentación, conocimiento o cualquier otro antecedente de nuestra propiedad, que sea puesto a su disposición o tuviera acceso a los mismos, se entienden para todos los efectos legales como 'Información Confidencial', esto es, se obligan a mantener estricta confidencialidad, reserva y a no divulgar por ningún motivo o causa los contenidos de ellos, ni a utilizarla en su propio beneficio.

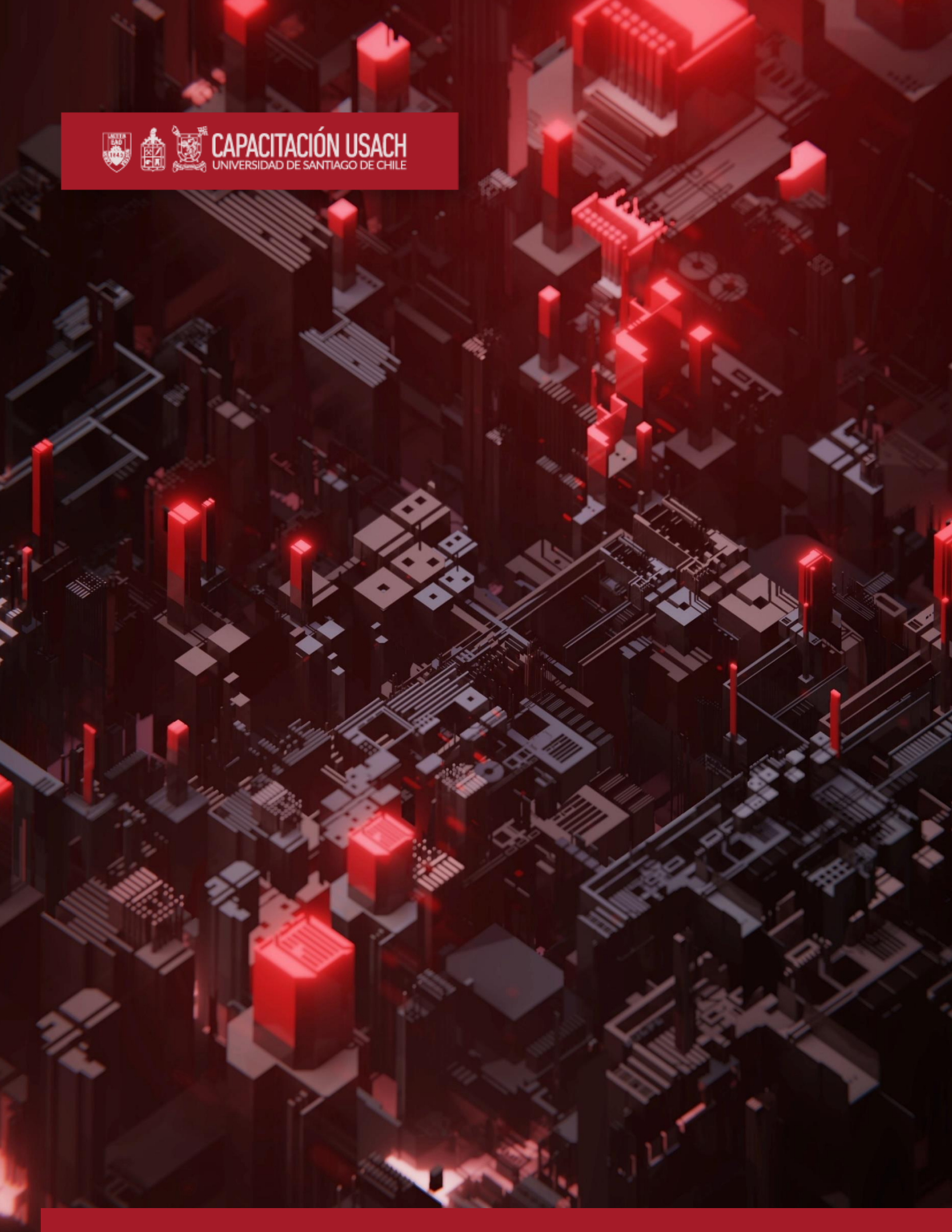
Esta obligación se hace extensiva a todos los funcionarios o empleados que formen parte de su empresa, sean o no dependientes, como también a sus socios y familiares. Lo anterior incluye tanto la información documentada como verbal.

La presente nota se entiende como parte esencial e integral de nuestra presentación del servicio.

Este documento se ha preparado para uso interno de NNNN por lo tanto, el y/o los lectores de éste, deben estar debidamente autorizados



**CAPACITACIÓN USACH**  
UNIVERSIDAD DE SANTIAGO DE CHILE



## Tabla de contenido

<b>ACUERDO DE CONFIDENCIALIDAD</b> .....	1
HISTORIAL DE CAMBIOS .....	1
<b>LISTA DE DISTRIBUCIÓN</b> .....	1
1.- REPORTE EJECUTIVO .....	2
1.1.- RESULTADOS OBTENIDOS .....	2
1.2.-IMPACTO.....	3

# Historial de Cambios

Autor		Revisado por	Aprobado por	Clasificación
Cristian Vera		Grupo 3	Grupo 3	Confidencial
Fecha Término Proyecto			Realizado Por	
24/09/2021			Cristian Vera	
Versión	Modificado por	Fecha Modificación	Observación	
1.0	Cristian Vera		Versión 1	
2.0	Sebastián Döll		Versión 2	
3.0	Cristian Vargas		Versión 3	
4.0	Cristian Muñoz		Versión 4	
5.0	Sebastián Holloway		Versión 5	

## Lista de distribución

Para	Accción	Empresa
Oscar Bravo	Lectura	USACH
Claudio Reyes	Lectura	USACH

## 1.- Reporte Ejecutivo

En el marco del proceso de auditoría de seguridad, USACH solicitó la revisión de los siguientes servidores:

192.168.0.2

192.168.0.3

Para 192.168.0.2 se encontraron los siguientes endpoints y servicios

- Servicio de FTP (Vsftpd)
- Máquinas vulnerables a ataques descritos por OWASP TOP 10

Para 192.168.0.3 se encontraron los siguientes endpoints:

<http://192.168.0.3/redteam>

### 1.1.- Resultados obtenidos

En el análisis de seguridad realizado al activo <http://192.168.0.3/redteam>, se detectaron cuatro vulnerabilidades relevantes, las cuales, de acuerdo a su nivel de riesgo se muestran a continuación:

ID	Vulnerabilidad	Estado	Criticidad
C1	SQL Injection	Activo	Critico
A1	LocalFile Inclusion	Activo	Alta
A2	XSS Reflejado	Activo	Alta
M1	HTML Injection	Activo	Media



## **1.2.-Impacto**

### **1.2.1.- SQL Injection**

La confidencialidad de la información se pierde debido a la filtración de información sensible dentro de la base de datos. La integridad de la información podría verse afectada si el atacante ingresara datos maliciosos a la base de datos.

### **1.2.1.- Local File Inclusion**

La confidencialidad de la información se pierde debido a que se pueden realizar consultas a archivos internos a la máquina. Sin embargo, la integridad y disponibilidad no se ven afectadas directamente.

### **1.2.3.- XSS Reflejado**

Es posible la ejecución del ataque en la página web lo cual afectaría la confidencialidad de la información entre el usuario y el servidor, sin embargo, la integridad y disponibilidad no se ven afectadas por este mismo. Aunque si un administrador es engañado podrían verse seriamente afectadas.

### **1.2.4.- HTML Injection**

Es posible la ejecución del ataque en la página web lo cual afectaría la confidencialidad de la información entre el usuario y el servidor, sin embargo, la integridad y disponibilidad no se ven afectadas por este mismo. Aunque si un administrador es engañado podrían verse seriamente afectadas.