

Implementación de Sistemas de seguridad en la empresa



Alumno: Arnau Vidal Millan

Curso: 2º ASIX

Instituto: IES Dr. Lluís Simarro

Tutor: Sergio Rey Martínez

Índice del proyecto

1. Introducción.....	4
1.1. Contextualización	4
2. Objetivos.....	7
3. Desarrollo del proyecto	8
3.1. Bitwarden	8
3.1.1. ¿Qué es Bitwarden?	8
3.1.2. Ventajas que nos ofrece Bitwarden	9
3.1.3. ¿Por qué se ha decidido sustituir el gestor de Google por Bitwarden?	10
3.1.4. Planes que nos ofrece Bitwarden.....	12
3.1.5. Configuraciones realizadas.....	14
3.1.5.1. Crear carpetas	15
3.1.5.2. Crear grupos	17
3.1.5.3. Políticas	20
3.1.6. Implementación de Bitwarden.....	23
3.1.6.1. Invitar usuarios	23
3.1.6.2. Crear cuenta de Bitwarden	25
3.1.6.3. Aceptar usuarios	26
3.1.6.4. Interfaz de Bitwarden	26
3.1.6.5. Agregar extensión al navegador	27
3.1.6.6. Guardar contraseñas	29
3.1.6.6.1. Manual.....	29
3.1.6.6.2. Automático	30
3.1.6.6.3. Importando contraseñas	30
3.1.6.7. Compartir contraseñas	31
3.2. Verificación de doble factor	33
3.2.1. ¿Cómo funciona?.....	33
3.2.2. Cuentas de Microsoft.....	34
3.2.2.1. Cómo configurar la verificación doble factor de Microsoft	34
3.2.3. VPN para teletrabajar	36

3.2.3.1. Cómo configurar la verificación doble factor para la VPN.....	36
3.3. Demostración del funcionamiento.....	38
3.3.1. BitWarden.....	38
3.3.2. Doble factor Microsoft	39
3.3.3. Doble factor VPN	40
4. Evaluación de los resultados	41
5. Conclusiones.....	44
6. Recursos utilizados	45
7. Tabla de ilustraciones	46
8. Bibliografía.....	48
9. Anexos.....	49

Introducción

La decisión de hacer este proyecto centrado en la implementación de sistemas de seguridad dentro de la empresa nace a raíz de que al llegar a Artesanía Cerda S.L., empresa donde he realizado las FCT, se tuvieron una serie de problemas que serán explicados en el siguiente punto.

Estos problemas representaban un riesgo potencial para la empresa, por tanto, se tomó la decisión de mejorar los sistemas de seguridad que se tenían en la empresa para así poder garantizar una mejor seguridad tanto a los trabajadores como a los datos de la empresa.

Antes de empezar con el proyecto me gustaría agradecer a Artesanía Cerdá S.L. por dejarme tomar capturas de pantalla sobre todo el proceso realizado y también quería aclarar que en algunas capturas de pantalla se verán algunos datos pixelados o tapados en blanco ya que desde la empresa me han pedido que mantenga oculta la identidad de cualquier trabajador.

Contextualización

El principal inconveniente mencionado anteriormente radica en que los empleados de nuestra empresa están almacenando todas las contraseñas en el gestor predeterminado de Google, una práctica que no cumple con los estándares de seguridad establecidos por la empresa. Esto plantea una preocupación seria en términos de seguridad de datos, ya que el almacenamiento de contraseñas en un servicio externo puede exponer nuestra información confidencial a riesgos innecesarios.

Por último, el segundo problema, y el más crítico de todos, es la detección de actividades sospechosas provenientes del correo electrónico de uno de nuestros empleados, identificadas a través del firewall corporativo.

Esta situación representa una grave amenaza para la seguridad de la empresa y sus datos sensibles.

<input type="checkbox"/>	16:06:00 2024-04-10	NEW	<div><div></div><div></div><div></div><div></div><div></div></div>		Anomaly	Account compromise detected in series of activities: login, login, New-InboxRule, login, login for user @cerdagroup.com Last activity from 45.93.59.54 (Spain)	Dismiss
<input type="checkbox"/>	14:00:19 2024-04-04	NEW	<div><div></div><div></div><div></div><div></div><div></div></div>		Anomaly	@cerdagroup.com was detected sending phishing emails strongly indicating their account is compromised. First email was Facturas 24150 - Working Spain	Dismiss Add Exception
<input type="checkbox"/>	13:58:11 2024-04-04	NEW	<div><div></div><div></div><div></div><div></div><div></div></div>		Anomaly	@cerdagroup.com has started a delete-all-emails inbox rule. This is often an indication that this account is taken over and used for launching email attacks.	Dismiss
<input type="checkbox"/>	13:24:54 2024-04-04	NEW	<div><div></div><div></div><div></div><div></div><div></div></div>		Anomaly	Detected suspicious login for user @cerdagroup.com from 35.198.79.70 (Germany). Detection reasons: legacy browser version (Edge 18.0), first login from country (Germany), logged in using hosting service (Google LLC), your users don't usually login from this network (Google LLC), recently logged in from multiple countries for the first time, recently logged in from multiple browsers for the first time, recently logged in from multiple VPN/hosting services for the first time	Dismiss
<input type="checkbox"/>	13:24:54 2024-04-04	NEW	<div><div></div><div></div><div></div><div></div><div></div></div>		Anomaly	Detected suspicious series of activities: login, login, login for user @cerdagroup.com Last activity from 35.198.79.70 (Germany)	Dismiss
<input type="checkbox"/>	13:17:34 2024-04-04	NEW	<div><div></div><div></div><div></div><div></div><div></div></div>		Anomaly	@cerdagroup.com performed geo-suspicious events: logged in from United Kingdom (51.195.195.102) and after 3 minutes logged in from Spain (45.93.59.54)	Dismiss Add Exception

ILUSTRACIÓN 1: ACTIVIDADES SOSPECHOSAS QUE DETECTA EL FIREWALL

Como se puede ver en la imagen anterior el firewall detectó varios inicios de sesión sospechosos desde Reino Unido y a los minutos detecto otro desde Alemania. Al darse cuenta de esto nos pusimos en contacto con el chico para que nos trajera el portátil ya que ese día él estaba teletrabajando.

También se puede ver en la imagen que el atacante creo una regla dentro del correo electrónico para que se borraran todos los correos existentes y, además, cualquier correo nuevo que le entrara se borraría automáticamente.

Finalmente, y lo peor de todo, el atacante envió facturas falsas a nombre de la empresa a 1500 direcciones de correo electrónico diferentes entre las que se encontraban clientes y proveedores de la empresa, pero gracias al firewall solo se llegaron a enviar 164 y ninguna de esas direcciones estaba registrada en la base de datos de la empresa.

Facturas 24150 - Working Spain



Para

@cerdagroup.com>

Cerdagroup

INVOICE SI-1833

TOTAL

€14,002.50

DUE DATE

01/27/2024

[View Invoice](#)

Salutations.



Finance & Accounting Technician

T: [+34 992 200 502](tel:+34992200502)@cerdagroup.com**ILUSTRACIÓN 2: CORREO QUE ENVÍA EL ATACANTE**

Después de lo ocurrido se envió un correo electrónico a esas 164 direcciones explicándoles que habíamos sido víctimas de un ataque de phishing.

Al no tener claro cómo el atacante consiguió el acceso al correo electrónico se decidió que teníamos que solucionar este problema de manera inmediata ya que después de lo ocurrido nos dimos cuenta de que los datos de la empresa y de los trabajadores no estaban protegidos.

Para solucionar estos problemas decidimos mejorar la seguridad, por tanto, optamos por implementar un nuevo gestor de contraseñas llamado Bitwarden y añadir la verificación de doble factor para Microsoft y para la VPN que utilizan los trabajadores para teletrabajar.

También se mandó un PowerPoint a todos los empleados donde se explicaba que es la ciberseguridad, como detectar diferentes tipos de ataques para así tener a todos los empleados mejor formados.

Este PowerPoint se podrá encontrar en el enlace de GitHub que se encuentra en el último apartado de la memoria.

Objetivos

Los objetivos de este proyecto son los siguientes:

- Configuración del gestor de contraseñas llamado Bitwarden
- Creación de carpetas organizadas por departamentos
- Creación de usuarios organizados por departamentos
- Explicar el funcionamiento del programa a todos los empleados de la empresa

Finalmente, los objetivos más importantes de este proyecto son:

- Implementación del gestor de contraseñas a todos los empleados de la empresa
- Implementación de la verificación doble factor de Microsoft a todos los empleados de la empresa
- Implementación de la verificación doble factor para la VPN a todos los empleados de la empresa

Todos estos objetivos en conjunto hacen el objetivo que quiere conseguir la empresa:

- Aumentar la seguridad de los trabajadores y de los datos de la empresa

Desarrollo del proyecto

Una vez ya hemos decidido que soluciones vamos a utilizar para mejorar la seguridad nos podemos poner con el proceso de implementación de estas mismas.

Bitwarden

¿Qué es Bitwarden?

Bitwarden es un gestor de contraseñas libre y de código abierto que ofrece una forma segura y conveniente de almacenar y gestionar tus credenciales en línea. Puede almacenar y gestionar inicios de sesión, tarjetas de crédito, identidad del usuario y notas seguras. Además, Bitwarden rellena automáticamente sus credenciales, lo que facilita y agiliza el proceso de inicio de sesión en varios sitios web y aplicaciones.



ILUSTRACIÓN 3: LOGO BITWARDEN

Bitwarden ofrece un servicio alojado en la nube y también posee la habilidad de implementar soluciones en software local.

Una de las herramientas más valiosas de Bitwarden es su generador de contraseñas seguras. Esta función crea contraseñas fuertes y únicas para cada uno de sus inicios de sesión, reduciendo el riesgo de ataques cibernéticos y compromisos de seguridad.



ILUSTRACIÓN 4: NUBE ENCRYPTADA

El servicio está disponible en interfaz web, aplicaciones de escritorio, complementos para navegador, aplicaciones móviles e interfaz de línea de comandos.

La manera más fácil para utilizar este gestor de contraseñas es instalar la extensión en su navegador favorito para una integración fácil o usar la aplicación de escritorio para una gestión de contraseñas más robusta y detallada.

Ventajas que nos ofrece Bitwarden

Estas son las ventajas que nos ofrece el gestor de contraseñas Bitwarden:

- Código abierto
- Desbloqueo biométrico
- Sincronización en la nube
- Guarda elementos como datos de usuario, notas seguras, tarjetas de crédito e identidades
- Cifrado de extremo a extremo de los datos de la caja fuerte
- Compartición segura de elementos de la caja fuerte con otros usuarios de Bitwarden
- Historial para poder consultar las contraseñas previas
- Autocompletado de información para iniciar sesión en páginas web y otras aplicaciones
- Generador de contraseñas
- Herramienta de comprobación de fortaleza de contraseñas
- Informes de fugas de datos y comprobación de contraseñas expuestas a través de Have I Been Pwned?
- Almacenamiento de claves TOTP (Time-based One-time Password) y generador de códigos
- Autenticación de múltiples factores a través de aplicaciones de autenticadores, correo electrónico, Duo, YubiKey y FIDO U2F
- Aplicaciones para múltiples plataformas.
- Servidor Bitwarden para alojar en servidor propio *on-premises*.
- Login con Single Sign-On.

¿Por qué se ha decidido sustituir el gestor de Google por Bitwarden?

Tras un exhaustivo análisis preliminar, se ha determinado que el gestor de contraseñas de Google presenta ciertas deficiencias en términos de seguridad, las cuales podrían ser subsanadas mediante la adopción de Bitwarden. A continuación, detallamos los problemas identificados:

1. Vulnerabilidades de seguridad en el navegador

Los navegadores web, por su naturaleza, están expuestos a una serie de amenazas en línea, que van desde malware hasta ataques de phishing y otros tipos de ataques cibernéticos. A pesar de que Google Chrome es conocido por su seguridad robusta, depender únicamente del navegador para almacenar contraseñas puede exponerte a riesgos si tu navegador se ve comprometido.

2. Falta de autenticación multifactorial

Bitwarden ofrece opciones para configurar la autenticación multifactorial, lo que agrega una capa adicional de seguridad para tus cuentas.

Google Chrome no proporciona una forma robusta de autenticación multifactorial para las contraseñas almacenadas. Esto significa que si un atacante logra acceder a tu navegador, potencialmente tendría acceso a todas tus cuentas guardadas sin necesitar una segunda forma de autenticación.

3. Sincronización en múltiples dispositivos

La sincronización en múltiples dispositivos en Bitwarden es segura y encriptada, lo que significa que tus contraseñas permanecen protegidas incluso cuando se sincronizan entre diferentes dispositivos.

Aunque la sincronización de contraseñas en Chrome es práctica y ahorra tiempo, también puede ser una fuente potencial de riesgo. Si tu cuenta de Google se ve comprometida, un atacante podría acceder a todas tus contraseñas sincronizadas en todos tus dispositivos, lo que podría tener consecuencias devastadoras.

4. Limitaciones en la generación de contraseñas seguras

Los gestores de contraseñas como Bitwarden ofrecen funcionalidades avanzadas, como la generación de contraseñas seguras y únicas para cada sitio web. Esto es crucial para evitar el uso de contraseñas débiles o repetidas, lo cual es una práctica común cuando se utilizan contraseñas almacenadas en el navegador.

5. Mayor control sobre tus contraseñas

Con un gestor de contraseñas, tienes un mayor control sobre tus credenciales. Puedes organizar, editar y eliminar contraseñas de manera fácil y segura. Además, muchos gestores de contraseñas ofrecen funciones adicionales, como el almacenamiento seguro de notas y otros datos confidenciales.

6. Código abierto y auditado

Bitwarden es un proyecto de código abierto, lo que significa que su código fuente es revisable por la comunidad para garantizar su seguridad. Esto proporciona una mayor transparencia y confianza en comparación con soluciones propietarias.

7. Encriptación de extremo a extremo

Todas las contraseñas y datos almacenados en Bitwarden están encriptados de extremo a extremo, lo que significa que incluso si los servidores de Bitwarden se ven comprometidos, tus datos permanecerán seguros.

En resumen, aunque Google Chrome ofrece una solución conveniente para el almacenamiento de contraseñas, no proporciona el nivel de seguridad y control que un gestor de contraseñas como Bitwarden puede ofrecer.



ILUSTRACIÓN 5: COMPARACIÓN BITWARDEN Y GOOGLE

Planes que nos ofrece Bitwarden

Bitwarden nos ofrece diferentes tipos de planes dependiendo del uso que le queramos dar. Le podemos dar dos usos diferentes a este gestor, uso personal y uso empresarial, dependiendo de esto nos ofrecerá unas características y unos precios diferentes.

Planes para uso personal:

- Gratis
 - 0€ al mes
 - Dispositivos ilimitados
 - Gestión de claves de acceso
 - Todas las funciones básicas
 - Compartir elementos del almacén con otros usuarios
- Premium
 - 1€ al mes
 - Mismas funciones que el gratis
 - Autenticador Bitwarden
 - Archivos adjuntos
 - Acceso de emergencia
 - Informes de seguridad y mucho más
- Familias
 - 3.33€ al mes
 - 6 cuentas premium
 - Compartir sin límites
 - Colectas ilimitadas
 - Organización del almacenamiento

Planes para uso empresarial:

- Equipos
 - 4€ al mes por usuario de la empresa
 - Funcionalidades premium
 - Comparta datos sensibles de manera segura con compañeros de trabajo, entre departamentos o con toda la empresa
- Empresa
 - 6€ al mes por usuario de la empresa
 - Funcionalidades premium
 - Políticas de empresa
 - SSO sin contraseña
 - Recuperación de cuentas
- Solicitar presupuesto
 - Funcionalidades premium
 - Con este plan se solicita un presupuesto personalizado que se adapta a la empresa según las características que se pidan, esto nos permite:
 - Reducir el riesgo en ciberseguridad
 - Aumentar la productividad
 - Integrarse perfectamente

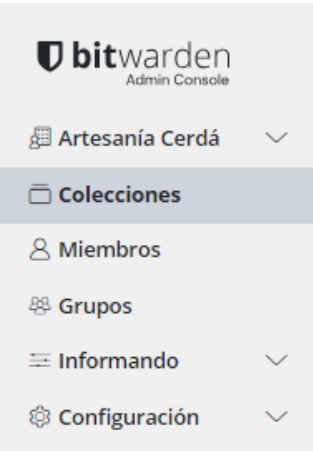
Configuraciones realizadas

Tras la realización del estudio sobre las características de Bitwarden y las ventajas que nos proporciona en función de los precios que ofrece, se procede a pedir un presupuesto personalizado para la empresa.

Una vez ya se tiene el servicio, se procede a la configuración de este siguiendo el siguiente árbol de carpetas:

- Artesanía Cerdá
 - Consumer Product Development
 - On Demand Product Development
 - Marketng
 - Digital Business
 - Data Analyst
 - Inbound
 - Export Sales
 - Iberit Sales
 - People & Talent
 - Production & Purchasing
 - Merchandiser
 - Purchases
 - Quality
 - Finance & Accounting
 - Supply Chain
 - Supply
 - Customer Succes
 - Logistics
 - Operarios Logistica
 - Sustainability
 - Supermoments

Crear carpetas



Para crear una carpeta debemos situarnos en Colecciones en el menú de la izquierda y arriba a la derecha nos aparecerá un botón azul que pone Nuevo y es un desplegable, en este desplegable escogemos la opción que dice Colección

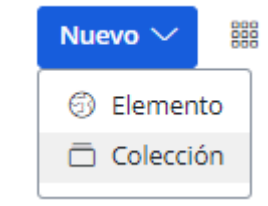


ILUSTRACIÓN 6: CREAR CARPETAS 1

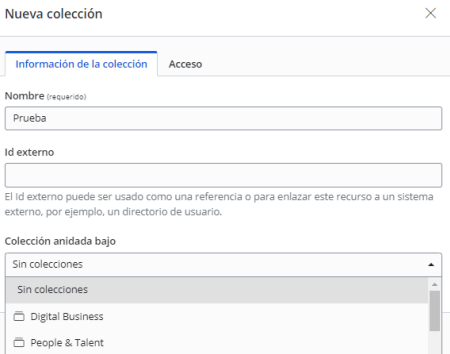


ILUSTRACIÓN 7: CREAR CARPETAS 2

Si queremos que una carpeta este por debajo de otra, lo que tenemos que hacer es crear primero la carpeta que esta por arriba y luego donde pone “colección anidada bajo” escogemos la carpeta que va por encima de esta que vamos a crear ahora

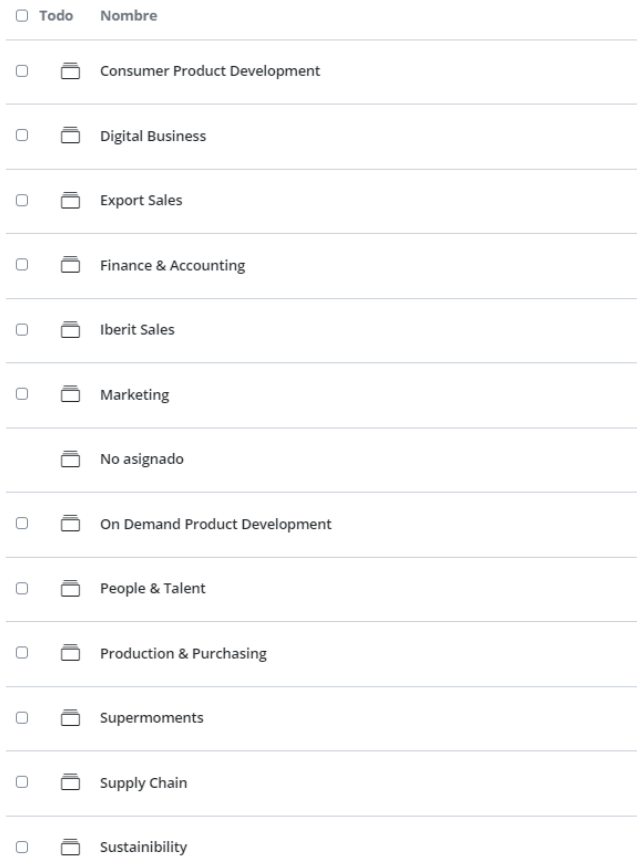


ILUSTRACIÓN 8: CARPETAS CREADAS 1

Capturas donde se ven que todas las carpetas están creadas (la carpeta de no asignado es una que viene por defecto y no se puede borrar):

Carpets dentro de Digital Bussines:

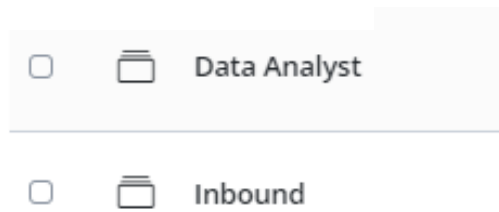


ILUSTRACIÓN 9: CARPETAS CREADAS 2

Carpets dentro de Supply Chain

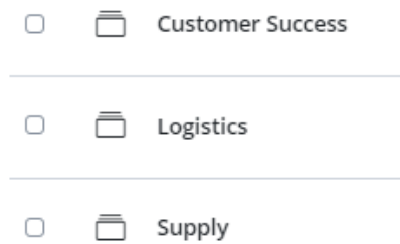


ILUSTRACIÓN 12: CARPETAS CREADAS 5

Carpets dentro de Production & Purchasing:

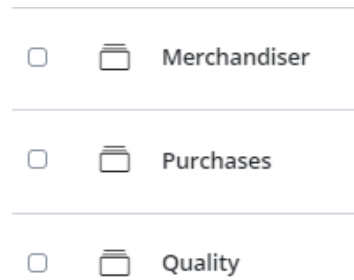


ILUSTRACIÓN 10: CARPETAS CREADAS 3

Carpeta dentro de Logistics:

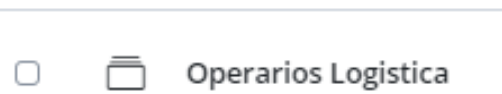
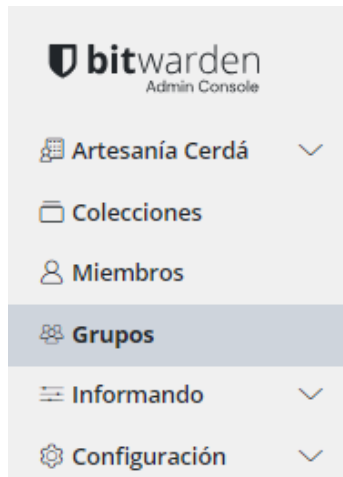


ILUSTRACIÓN 11: CARPETAS CREADAS 4

Crear grupos



Una vez ya tenemos todas las carpetas creadas podemos empezar a crear los grupos, estos grupos se llamarán igual que las carpetas que ya tenemos.

Para crear los grupos tenemos que ir al menú de la izquierda al igual que con las carpetas, pero esta vez pulsar sobre la opción que pone grupos y aquí dentro ir arriba a la derecha donde pone Nuevo grupo

+ Nuevo Grupo

ILUSTRACIÓN 13: CREAR GRUPOS 1

Al pulsar sobre Nuevo Grupo se nos abrirá una ventana donde tendremos que poner el nombre del grupo.

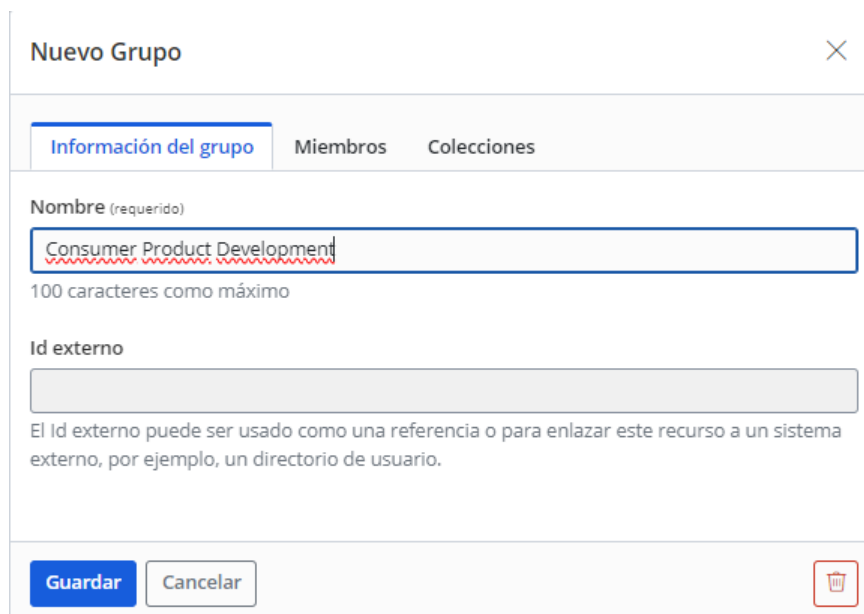


ILUSTRACIÓN 14: CREAR GRUPOS 2

Una vez tengamos ya el nombre nos iremos a la sección donde pone colecciones y aquí tendremos que poner en permiso “Puede gestionar” y luego seleccionaremos la colección que se llame igual que el grupo. Le ponemos estos permisos a los grupos para que todos los trabajadores que estén dentro de este grupo puedan compartir contraseñas en la colección donde están.

Nuevo Grupo

Información del grupo Miembros Colecciones

Conceder acceso a las colecciones añadiéndolas a este grupo.

Permiso: Puede gestionar

Colección: No hay colecciones añadidas

Guardar Cancelar

Seleccionar colecciones

Escriba para filtrar --

- Consumer Product Development
- Digital Business
- Digital Business/Data Analyst
- Digital Business/Inbound
- Export Sales
- Finance & Accounting
- Iberit Sales

ILUSTRACIÓN 15: CREAR GRUPOS 3

Una vez ya lo tengamos todo ya podemos darle al botón de guardar.

Captura donde se ven todos los grupos creados:

<input type="checkbox"/> Todo	Nombre	Colecciones
<input type="checkbox"/>	Consumer Product Development	Consumer Product Dev...
<input type="checkbox"/>	Customer Success	Supply Chain/Custome...
<input type="checkbox"/>	Data Analyst	Digital Business/Data ...
<input type="checkbox"/>	Digital Business	Digital Business
<input type="checkbox"/>	Export Sales	Export Sales
<input type="checkbox"/>	Finance & Accounting	Finance & Accounting
<input type="checkbox"/>	Iberit Sales	Iberit Sales
<input type="checkbox"/>	Inbound	Digital Business/inbou...
<input type="checkbox"/>	Logistics	Supply Chain/Logistics Supply Chain/Logistics...
<input type="checkbox"/>	Marketing	Marketing
<input type="checkbox"/>	Merchandiser	Production & Purchasi...
<input type="checkbox"/>	On Demand Product Development	On Demand Product D...
<input type="checkbox"/>	Operarios Logistica	Supply Chain/Logistics...
<input type="checkbox"/>	People & Talent	People & Talent
<input type="checkbox"/>	Production & Purchasing	Production & Purchasing Production & Purchasi... + 2 más
<input type="checkbox"/>	Purchases	Production & Purchasi...
<input type="checkbox"/>	Quality	Production & Purchasi...
<input type="checkbox"/>	Supermoments	Supermoments
<input type="checkbox"/>	Supply	Supply Chain/Supply
<input type="checkbox"/>	Supply Chain	Supply Chain Supply Chain/Custome... + 3 más
<input type="checkbox"/>	Sustainability	Sustainability

ILUSTRACIÓN 16: GRUPOS CREADOS

En el caso de Supply Chain, Production & Purchasing y Logistics cuando creamos el grupo en el apartado de colecciones tendremos que poner también que puedan gestionar las carpetas que están por debajo de la suya ya que los permisos no se heredan en las carpetas que están en un nivel inferior.





Permiso		Seleccionar colecciones	
Puede ver ▼		-- Escriba para filtrar -- ▼	
Colección		Permiso	
 Production & Purchasing		Puede gesti... ▼	×
 Production & Purchasing/Merchandise		Puede gesti... ▼	×
 Production & Purchasing/Purchases		Puede gesti... ▼	×
 Production & Purchasing/Quality		Puede gesti... ▼	×

ILUSTRACIÓN 19: PERMISOS PRODUCTION & PURCHASING






Colección		Permiso	
 Supply Chain		Puede gesti... ▼	×
 Supply Chain/Customer Success		Puede gesti... ▼	×
 Supply Chain/Logistics		Puede gesti... ▼	×
 Supply Chain/Logistics/Operarios Logística		Puede gesti... ▼	×
 Supply Chain/Supply		Puede gesti... ▼	×

ILUSTRACIÓN 18: PERMISOS SUPPLY CHAIN



Permiso		Seleccionar colecciones	
Puede ver ▼		-- Escriba para filtrar -- ▼	
Colección		Permiso	
 Supply Chain/Logistics		Puede gesti... ▼	×
 Supply Chain/Logistics/Operarios Logística		Puede gesti... ▼	×

ILUSTRACIÓN 17: PERMISOS LOGISTICS

Políticas

Una vez ya tenemos todos los grupos creados solo nos queda configurar unas políticas.

Para empezar con la configuración de estas políticas nos tendremos que abrir el apartado de configuración que aparece en el menú de la izquierda y pulsar sobre el apartado que dice políticas.

En nuestro caso necesitaremos activar las siguientes cuatro políticas:

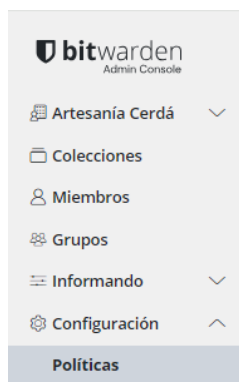


ILUSTRACIÓN 20:
POLÍTICAS 1



ILUSTRACIÓN 21: POLÍTICAS 2

La primera política sirve para especificar unos requisitos en la contraseña, para ello nos meteremos dentro, marcaremos la casilla donde pone Activar y le especificaremos los siguientes requisitos:

- Mínimo de 12 caracteres
- Mínimo una mayúscula
- Mínimo una minúscula
- Mínimo un número
- Mínimo un carácter especial de los que se ve en la imagen

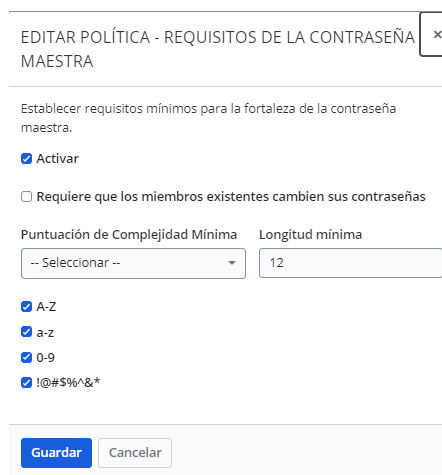


ILUSTRACIÓN 22: POLÍTICA CONTRASEÑAS

La segunda política sirve para que los usuarios puedan autorizar a los administradores para poder cambiarles la contraseña ya que por defecto la contraseña no se puede cambiar.

Una vez estamos dentro de la política tendremos que marcar las dos opciones que nos aparecen.

La primera opción que nos aparece es para activarlo y la segunda es para que los usuarios automáticamente estén inscritos.



ILUSTRACIÓN 23: POLÍTICA RECUPERAR CUENTA 1

Si no marcamos esta segunda opción los usuarios deberían ir a su caja fuerte y en el apartado donde les sale el nombre de la organización pulsarían en los puntos que aparecen a la derecha y pulsar en la opción que dice “Inscribirse en la recuperación de la cuenta”.

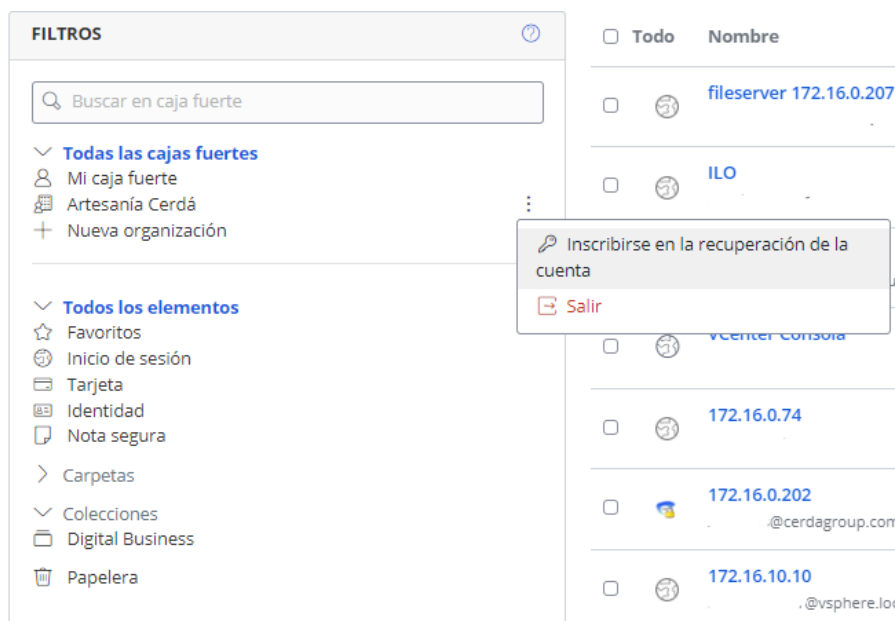


ILUSTRACIÓN 24: POLÍTICA RECUPERACIÓN CUENTA 2

Una vez ya estén aquí dentro les aparecerá una ventana que les pedirá que pongan la contraseña y al darle al botón de enviar ya estarían inscritos en la recuperación de la cuenta.

Si en el perfil del usuario no sale la llave a la derecha es que ya estamos inscritos.

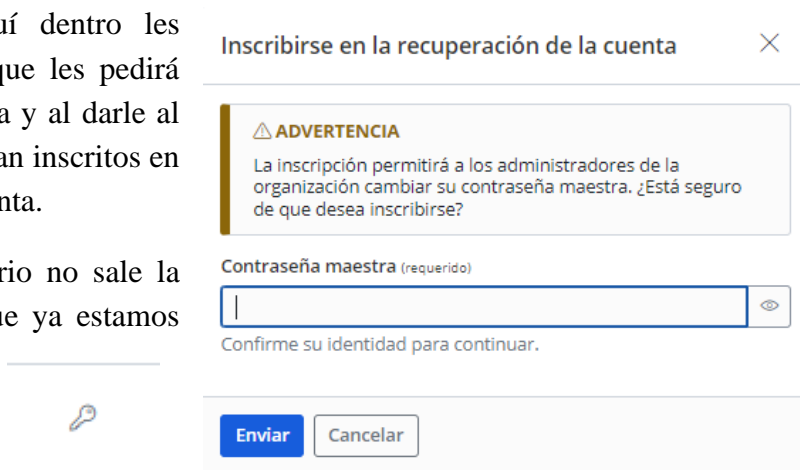


ILUSTRACIÓN 25: POLÍTICA RECUPERACIÓN CUENTA 3

EDITAR POLÍTICA - GENERADOR DE CONTRASEÑAS ×

Establecer requisitos mínimos para la configuración del generador de contraseñas.

☒ Activar

Tipo por defecto

Preferencia de usuario ▼

CONTRASEÑA

Longitud mínima

12

Mínimo de caracteres numéricos

1

Mínimo de caracteres especiales

1

☒ A-Z

☒ a-z

☒ 0-9

☒ !@#\$%^&*

FRASE DE CONTRASEÑA

Número mínimo de palabras

☐ Capitalizar

☐ Incluir número

Guardar

Cancelar

ILUSTRACIÓN 26: POLÍTICA GENERADOR DE CONTRASEÑAS

Y finalmente la última política que tenemos que activar es la política de organización única.

Esta política lo que hace es restringir a los usuarios que no son administradores para que no puedan unirse a una organización distinta y solo estén en la organización de la empresa.

La tercera política que tenemos que activar es un generador de contraseñas seguras.

Al activar esta política podremos generar contraseñas seguras, estas contraseñas seguras cumplirán unos requisitos mínimos que previamente le hemos establecido.

Los requisitos son:

- Mínimo de 12 caracteres
- Mínimo una mayúscula
- Mínimo una minúscula
- Mínimo un número
- Mínimo un carácter especial

EDITAR POLÍTICA - ORGANIZACIÓN ÚNICA ×

Restringir a los usuarios de ser capaces de unirse a otras organizaciones.

⚠ ADVERTENCIA

Los miembros de la organización que no son dueños o administradores y que ya son miembros de otra organización serán eliminados de su organización.

☒ Activar

Guardar

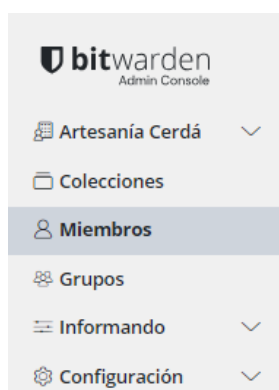
Cancelar

ILUSTRACIÓN 27: POLÍTICA ORGANIZACIÓN ÚNICA

Implementación de Bitwarden

Una vez ya tenemos el servicio configurado de la manera que se nos pide ya podemos empezar con la implementación de este gestor de contraseñas a todos los trabajadores de la empresa.

Invitar usuarios



Para empezar con la implementación del servicio hay que invitar a los usuarios, para ello, pulsaremos sobre Miembros en el menú de la izquierda y dentro de esta sección, arriba a la derecha nos aparecerá un botón donde dice “Invitar miembro”

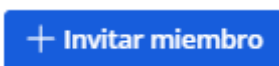


ILUSTRACIÓN 28: INVITAR USUARIOS 1

Al pulsar sobre este botón se nos abrirá una ventana donde tendremos que especificar el rol, el correo electrónico y el grupo al que pertenece este usuario.

En el apartado de colecciones no seleccionaremos nada ya que anteriormente, cuando creamos los grupos, ya les pusimos los permisos sobre las carpetas, por tanto, aquí no hace falta especificar ningún permiso.

ILUSTRACIÓN 29: INVITAR USUARIOS 2

Una vez tengamos toda la información pulsaremos sobre el botón de invitar. Al pulsar sobre el botón de invitar llegará un correo de Bitwarden a la dirección de correo electrónico que hemos puesto anteriormente, dentro de este correo se encuentra una invitación para unirse a la organización.

Foto del correo de invitación:

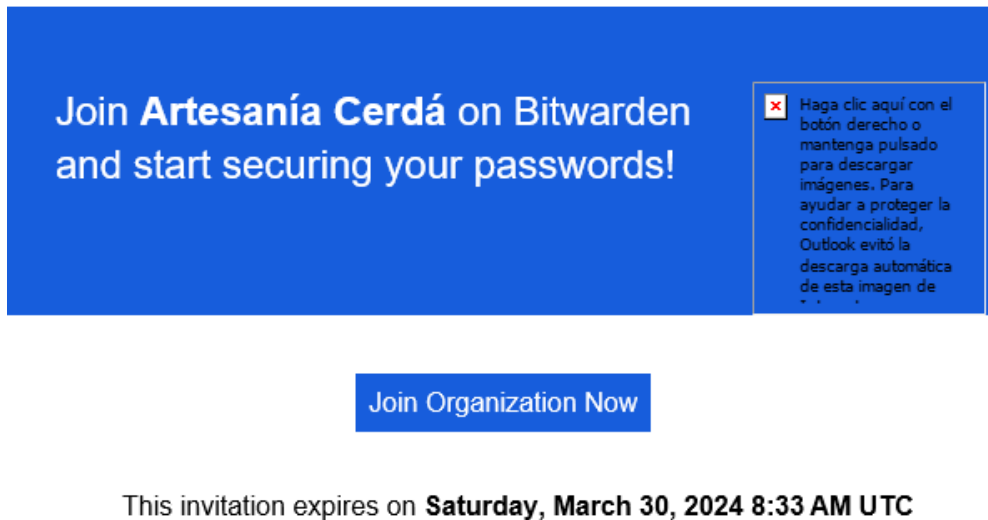


ILUSTRACIÓN 30: CORREO DE INVITACIÓN

Crear cuenta de Bitwarden

Al pulsar sobre el botón azul que dice "Join organization now" se nos abrirá una ventana en el navegador donde tendremos que crearnos una cuenta en Bitwarden..

Arriba del apartado de contraseña se puede ver que aparece una ventana de texto donde aclara los requisitos que debe cumplir la contraseña.

Una vez ya tengamos completos todos los campos, marcaremos la casilla donde dice que aceptamos los términos y ya podríamos crear la cuenta.

Al crear la cuenta el navegador nos redirigirá a la ventana de iniciar sesión de Bitwarden donde introduciremos nuestras credenciales para el inicio de sesión.

Debemos tener en cuenta que abajo donde pone servidor tenemos que estar en bitwarden.eu, si tenemos cualquier otra opción intentaremos iniciar sesión y nos dirá que nuestra contraseña es incorrecta.

Correo electrónico (requerido)

Utilizarás tu correo electrónico para acceder.

Nombre

¿Cómo deberíamos llamarte?

Una o más políticas de la organización requieren que su contraseña maestra cumpla con los siguientes requisitos:

- Longitud mínima 12
- Contiene uno o más caracteres en mayúsculas
- Contiene uno o más caracteres en minúsculas
- Contiene uno o más números
- Contienen uno o más de los siguientes caracteres especiales !@#\$%^&*

Contraseña maestra (requerido)

Importante: ¡Las contraseñas maestras no pueden ser recuperadas si las olvidas! 12 caracteres mínimo

Vuelve a escribir tu contraseña maestra (requerido)

Pista de contraseña maestra

Una pista de tu contraseña maestra puede ayudarte a recordarla en caso de que la olvides.

☒ Comprobar filtración de datos conocidas para esta contraseña

☐ Al seleccionar esta casilla, acepta lo siguiente:
[Términos y condiciones del servicio](#), [Política de privacidad](#)

Crear cuenta

ILUSTRACIÓN 31: CREAR CUENTA EN BITWARDEN

Correo electrónico (requerido)

☒ Recordar correo electrónico

Continuar

o

[Iniciar sesión con la clave de acceso](#)

¿Nuevo por aquí? [Crear cuenta](#)

Servidor: [bitwarden.eu](#)

Contraseña maestra (requerido)

[Obtener pista de la contraseña maestra](#)

Iniciar sesión con contraseña maestra

ILUSTRACIÓN 32: INICIAR SESIÓN EN BITWARDEN

Aceptar usuarios

Al iniciar sesión por primera vez el administrador recibirá un correo para que nos acepte en la organización.

En caso de ser los administradores de la organización para aceptar a alguien nos dirigiremos al menú de la izquierda, pulsaremos donde pone miembros y dentro de miembros nos iremos al apartado de Necesita confirmación y aceptaremos a todos los usuarios que estén pendientes.

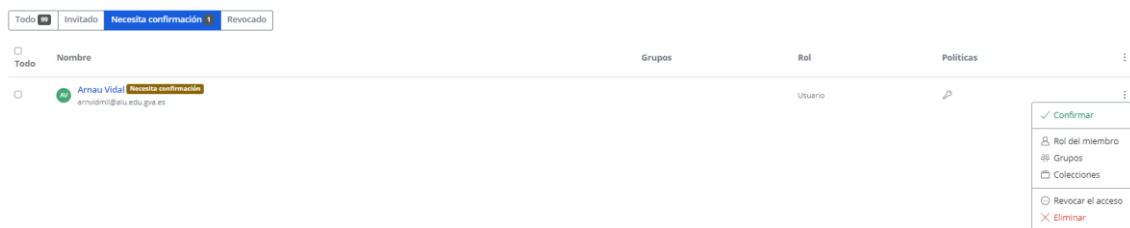


ILUSTRACIÓN 33: ACEPTAR USUARIOS EN BITWARDEN

Interfaz de Bitwarden

Cuando ya estemos aceptados dentro de la organización veremos la página web de la siguiente manera:

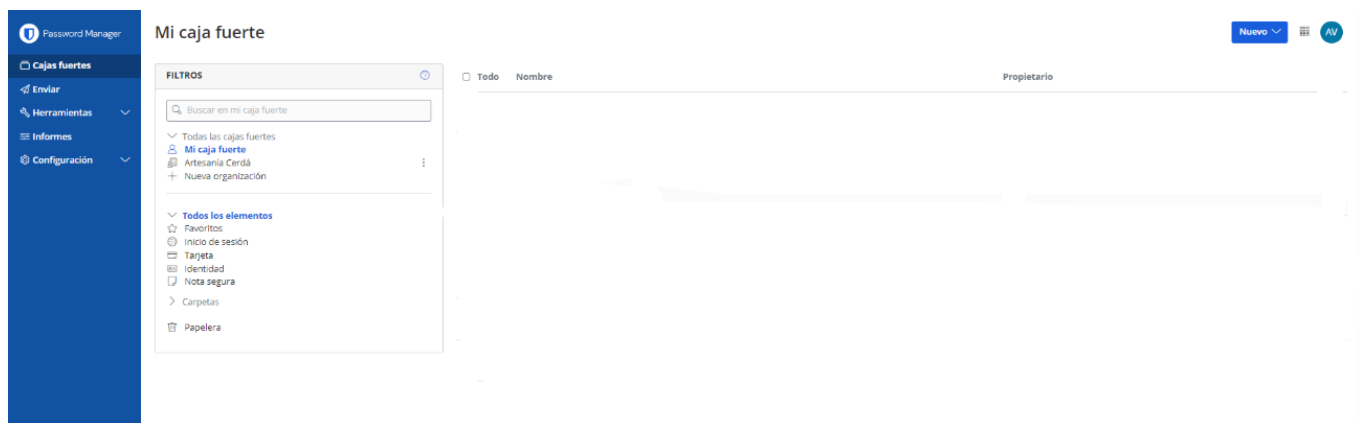


ILUSTRACIÓN 34: CAJA FUERTE

Como se puede ver en el menú blanco que hay a la derecha del menú azul ahora mismo estamos en nuestra caja fuerte, aquí es donde se guardaran todas las contraseñas por defecto y abajo nos sale el nombre de la organización que es donde podremos compartir contraseñas para que la gente que se encuentra en la misma colección y grupo que nosotros puedan verlas.

Agregar extensión al navegador

Después de iniciar sesión por primera vez necesitamos añadir la extensión de Bitwarden a nuestro navegador, esta extensión nos permitirá tener un acceso más rápido a Bitwarden.

Para añadir la extensión a nuestro navegador nos iremos arriba a la derecha donde aparecen unos puntitos debajo de la X para cerrar la ventana, aquí dentro nos iremos a Extensiones → Visitar Chrome Web Store

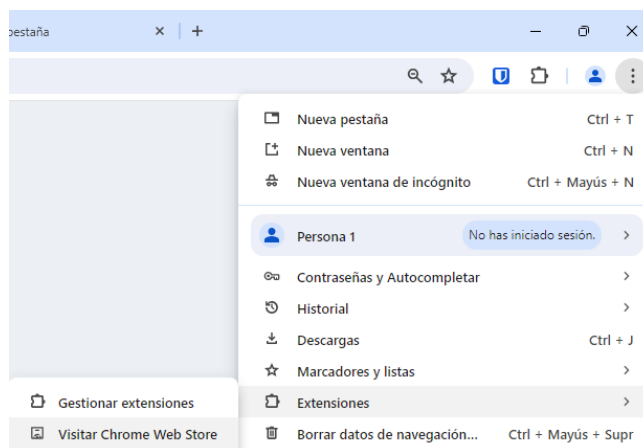


ILUSTRACIÓN 35: AGREGAR EXTENSIÓN 1

Al pulsar sobre Visitar Chrome Web Store se nos abrirá una ventana donde tendremos que buscar Bitwarden y luego añadir la extensión, en mi caso aparece Desinstalar porque ya tengo esta extensión.



Desinstalar

ILUSTRACIÓN 36: AGREGAR EXTENSIÓN 2

Después de añadir la extensión tenemos que anclarla al navegador. Para ello, nos volvemos arriba a la derecha, a la izquierda de los tres puntos donde hemos ido antes para añadir la extensión, y aquí nos aparece un símbolo que es una pieza de un puzzle que pone extensiones, pulsamos sobre este símbolo, nos situamos sobre Bitwarden y pulsamos sobre el botón que dice Fijar. Al tener la extensión fijada nos aparecerá el símbolo de Bitwarden a la izquierda de el de las extensiones.

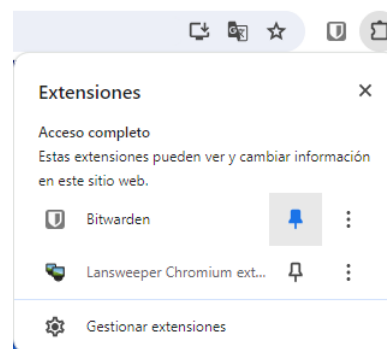


ILUSTRACIÓN 37: AGREGAR EXTENSIÓN 3

Finalmente, solo nos quedaría iniciar sesión desde la extensión, para ello pulsamos sobre el icono de Bitwarden y se nos abrirá la siguiente ventana.

Al igual que cuando hemos iniciado sesión anteriormente debemos tener en cuenta el servidor donde vamos a iniciar sesión y poner bitwarden.eu.

Si tenemos Bitwarden.com al igual que en la foto no nos dejara entrar a nuestra cuenta.

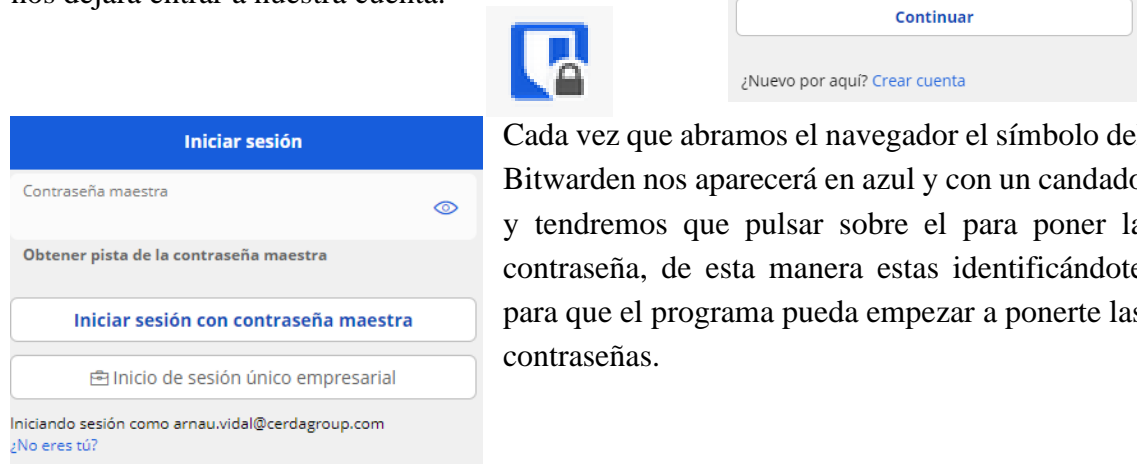


ILUSTRACIÓN 38: AGREGAR EXTENSIÓN 4

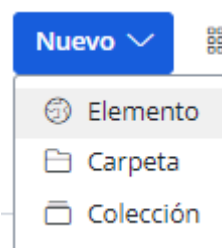
Guardar contraseñas

Para guardar contraseñas hay tres maneras distintas de hacerlo:

- Manual
- Automático
- Importando contraseñas

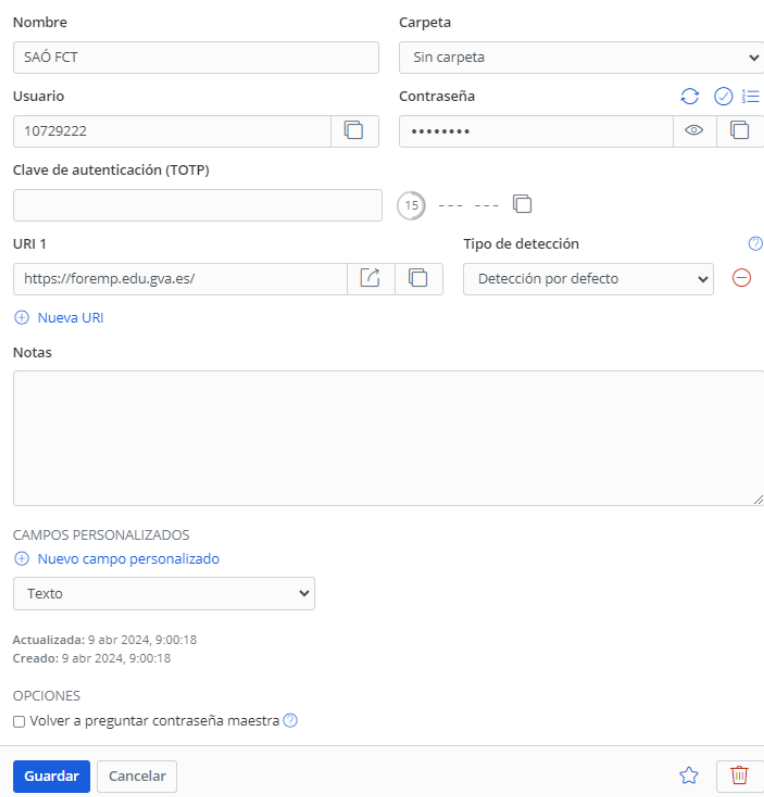
Manual

Para añadir una contraseña de manera manual debemos irnos a la página web donde podemos ver nuestra caja fuerte y arriba a la derecha nos aparecerá un botón azul que pone nuevo, pulsaremos sobre él y escogeremos Elemento.



Al crear un nuevo elemento se nos abrirá la siguiente ventana donde tendremos que rellenar los datos del inicio de sesión.

Nos pedirá poner nombre, usuario, contraseña y el enlace de la página web.



The form contains the following fields and sections:

- Nombre:** Text input with value "SAÓ FCT".
- Carpeta:** Dropdown menu with value "Sin carpeta".
- Usuario:** Text input with value "10729222".
- Contraseña:** Password input field with masked characters "*****".
- Clave de autenticación (TOTP):** Text input with a circular icon containing "15".
- URI 1:** Text input with value "https://foremp.edu.gva.es/".
- Tipo de detección:** Dropdown menu with value "Detección por defecto".
- Notas:** Large text area for notes.
- CAMPOS PERSONALIZADOS:** Section with a dropdown menu showing "Nuevo campo personalizado" and "Texto".
- Actualizada:** 9 abr 2024, 9:00:18.
- Creado:** 9 abr 2024, 9:00:18.
- OPCIONES:** Section with a checkbox "Volver a preguntar contraseña maestra" (checked).
- Buttons:** "Guardar" (blue), "Cancelar", "Favoritos" (star icon), and "Eliminar" (trash icon).

Una vez tengamos todos los datos rellenados le daremos al botón de guardar.

ILUSTRACIÓN 39: AGREGAR CONTRASEÑA DE FORMA MANUAL

Automático

Para agregar una contraseña de manera automática solo tendremos que iniciar sesión en la página donde queramos guardar esas credenciales y nos aparecerá el siguiente recuadro a la parte superior de nuestro navegador.



ILUSTRACIÓN 40: AGREGAR CONTRASEÑA DE FORMA AUTOMÁTICA

Al pulsar sobre el botón azul que dice “sí, guardar ahora” estas credenciales se guardarían automáticamente en nuestra caja fuerte.

Importando contraseñas

Si queremos importar las credenciales que tenemos guardadas en el gestor de Google tendremos que dirigirnos a los puntos de arriba a la derecha → Contraseñas y Autocompletar → Gestor de Contraseñas de Google.

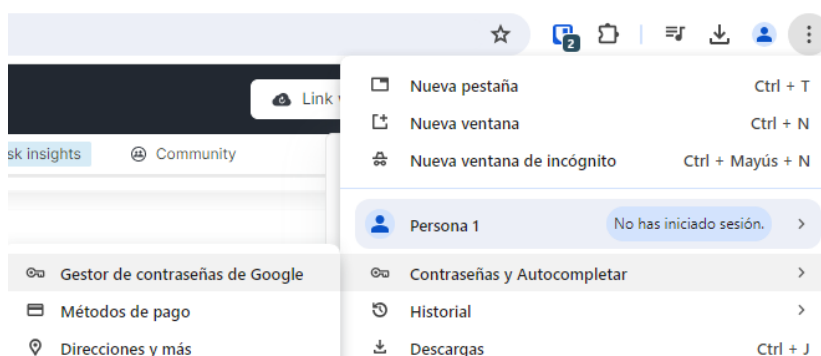


ILUSTRACIÓN 41: AGREGAR CONTRASEÑAS IMPORTÁNDOLAS 1

Dentro de esta ventana pulsaremos sobre el icono de configuración en el menú de la izquierda y en el apartado de configuración pulsaremos sobre el botón que dice Descargar archivo.

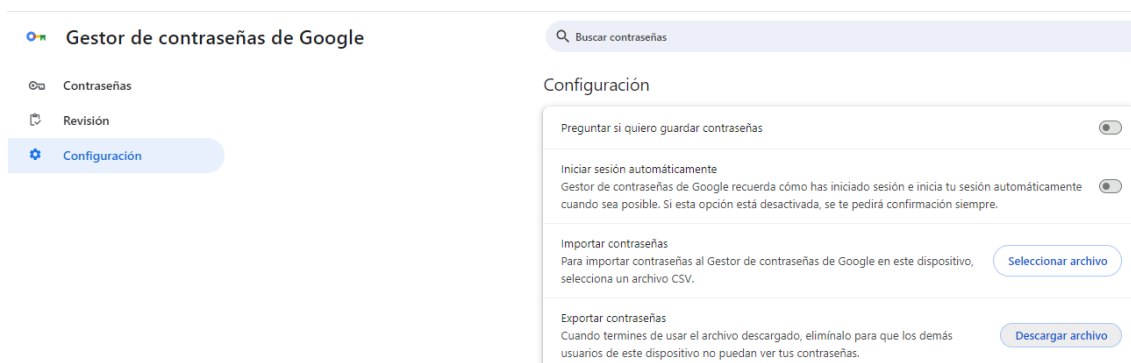


ILUSTRACIÓN 42: AGREGAR CONTRASEÑAS IMPORTÁNDOLAS 2

Finalmente, una vez tengamos el archivo descargado nos dirigiremos a nuestra Caja fuerte y en el menú azul de la izquierda nos iremos a Herramientas → Importar datos

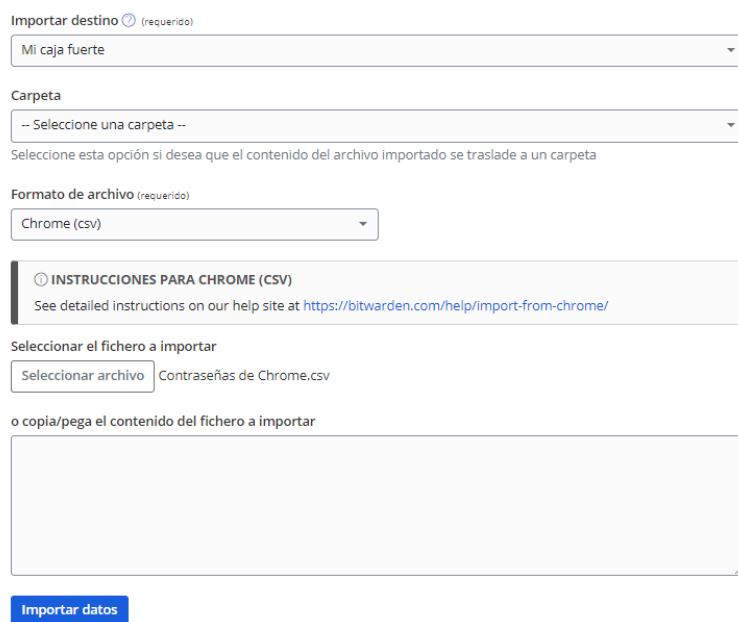
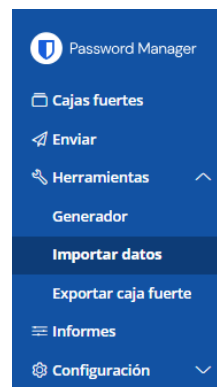


ILUSTRACIÓN 43: AGREGAR CONTRASEÑAS IMPORTÁNDOLAS 3

Aquí dentro tendremos que escoger el formato del archivo que en mi caso es Chrome (csv) y seleccionar el archivo que queremos importar, cuando este todo le daríamos al botón azul y ya tendríamos todas las contraseñas importadas.



Compartir contraseñas

Para compartir una contraseña debemos situarnos sobre los puntos que nos salen a la derecha y escoger la opción que dice mover a la organización.

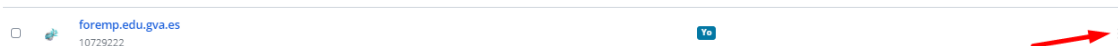
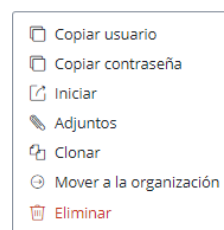


ILUSTRACIÓN 44: COMPARTIR CONTRASEÑA 1

Al clicar sobre mover a la organización se nos abrirá una ventana donde tendremos que seleccionar a que colección queremos mover esta contraseña, en mi caso solo aparece Digital Bussines ya que solo formo parte de ese departamento.



MOVER A LA ORGANIZACIÓN foremp.edu.gva.es

Elige una organización a la que deseas mover este objeto. Moviendo a una organización transfiere la propiedad del objeto a esa organización. Ya no serás el dueño directo de este objeto una vez que haya sido movido.

Organización

Artesanía Cerdá

COLECCIONES

[Seleccionar todo](#)

[Deseleccionar todo](#)

☐ Digital Business

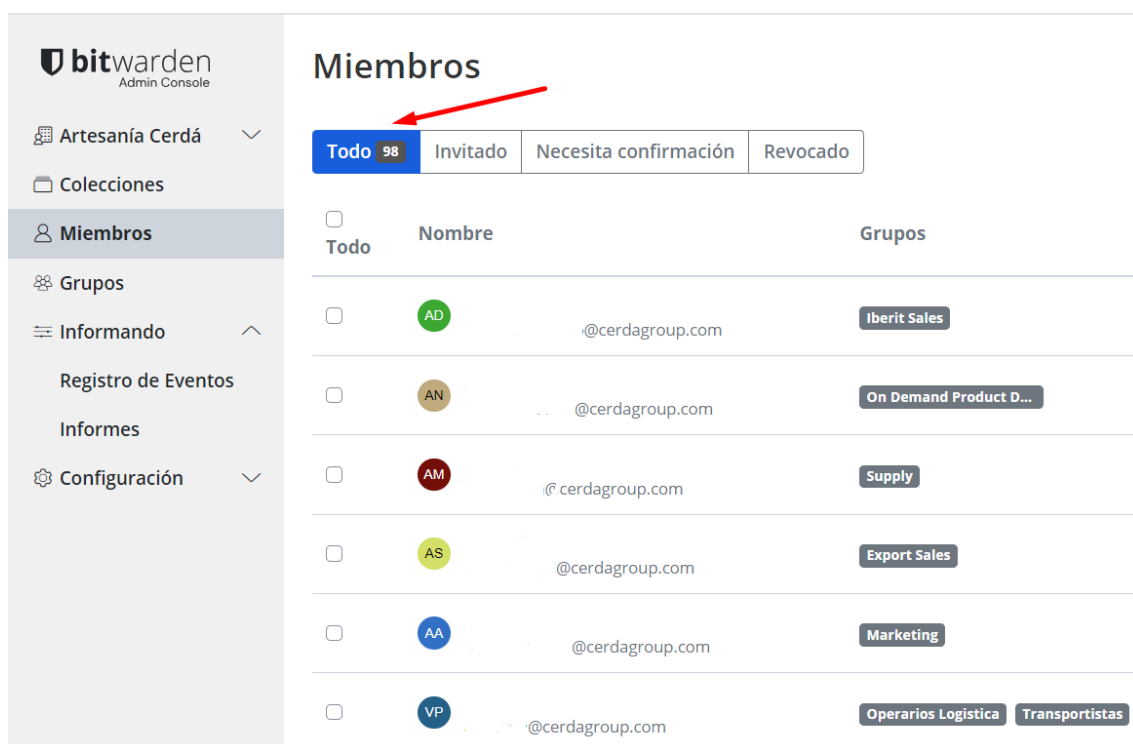
Guardar

Cancelar

Al darle al botón de guardar la contraseña pasaría de estar en nuestra caja fuerte a estar en Artesanía Cerdá que es nuestra organización, desde aquí cualquier usuario que esté en el grupo de Digital Business podrá ver, utilizar y modificar esta contraseña.

ILUSTRACIÓN 45: COMPARTIR CONTRASEÑA 2

Después de haber hecho todo este proceso con noventa y ocho trabajadores que hay en las oficinas de la empresa la siguiente captura demuestra que todos los empleados están dentro de la organización en Bitwarden.



bitwarden
Admin Console

Artesanía Cerdá

Colecciones

Miembros

Grupos

Informando

Registro de Eventos

Informes

Configuración

Miembros

Todo 98 Invitado Necesita confirmación Revocado

	Nombre	Grupos
<input type="checkbox"/>	AD @cerdagroup.com	Iberit Sales
<input type="checkbox"/>	AN @cerdagroup.com	On Demand Product D...
<input type="checkbox"/>	AM @cerdagroup.com	Supply
<input type="checkbox"/>	AS @cerdagroup.com	Export Sales
<input type="checkbox"/>	AA @cerdagroup.com	Marketing
<input type="checkbox"/>	VP @cerdagroup.com	Operarios Logística Transportistas

ILUSTRACIÓN 46: USUARIOS DENTRO DE LA ORGANIZACIÓN

Verificación de doble factor

El doble factor de autenticación, también conocido como 2FA, es una medida de seguridad que sirve para verificar la identidad de la persona que quiere ingresar a una cuenta.

El doble factor de autenticación añade una segunda capa de protección, reforzando el nivel de seguridad de nuestras cuentas de usuario y de nuestros datos personales. Esto lo logra utilizando dos métodos distintos para validar nuestra identidad.

El primer método generalmente es una contraseña segura, y el segundo método podría ser un código obtenido a través de un correo electrónico o un mensaje de texto, reconocimiento facial, entre otros.

¿Cómo funciona?

Existen diversas maneras en las que se puede lograr esta capa adicional de seguridad. Sin embargo, todos los métodos logran lo mismo y cumplen con ciertas generalidades. El funcionamiento típico de estos sistemas es el siguiente:

- Primero, se accede a un servicio o plataforma en línea y se ingresa la contraseña. Este es el primer factor de autenticación.
- A continuación, el servicio en línea solicita un segundo factor de autenticación, que puede ser un código de verificación que envía por correo electrónico, una huella dactilar, u otro método que se configure previamente.

Finalmente, se proporciona ese segundo factor de autenticación para verificar la identidad del dueño de la cuenta y completar el inicio de sesión.



ILUSTRACIÓN 47: VERIFICACIÓN DOBLE FACTOR

Cuentas de Microsoft

El doble factor de autenticación de Microsoft consiste en que cada vez que se intente iniciar sesión en un dispositivo que no es de confianza, después de poner la contraseña aparecerá un número en la pantalla, este número tendremos que ponerlo dentro de la aplicación de Microsoft authenticator.

Con esto hacemos que solo nosotros podamos acceder a nuestra cuenta ya que somos los únicos que podremos introducir el número en la aplicación del móvil.

Cómo configurar la verificación doble factor de Microsoft

Para empezar a configurar la verificación doble factor de Microsoft debemos instalarnos la Aplicación Microsoft Authenticator en el móvil.

Una vez ya tenemos la aplicación instalada debemos irnos a este enlace <https://mysignins.microsoft.com/security-info>



Dentro de este enlace tendremos que pulsar sobre el botón que dice “Agregar un método de inicio de sesión” y en el desplegable que se nos abre elegir Aplicación de autenticación.

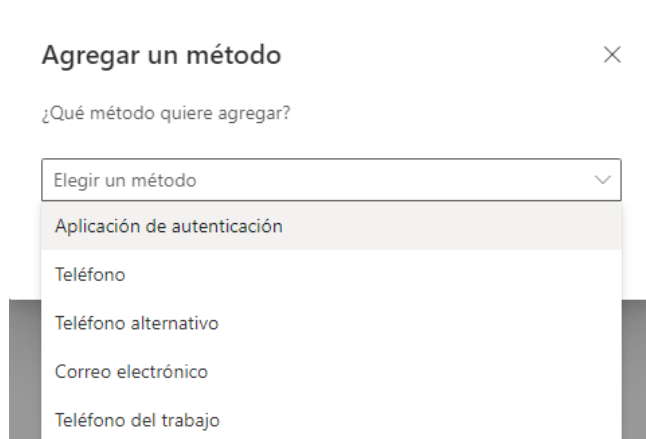
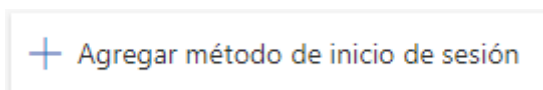


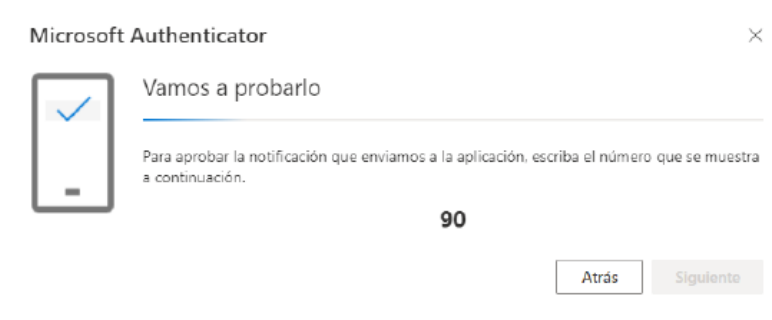
ILUSTRACIÓN 49: CONFIGURAR DOBLE FACTOR MICROSOFT 1

Una vez escogido el método de inicio de sesión tendremos que darle a siguiente hasta que nos aparezca en pantalla un código QR, este código lo tendremos que escanear con la aplicación de Microsoft Authenticator.



ILUSTRACIÓN 50: CONFIGURAR DOBLE FACTOR MICROSOFT 2

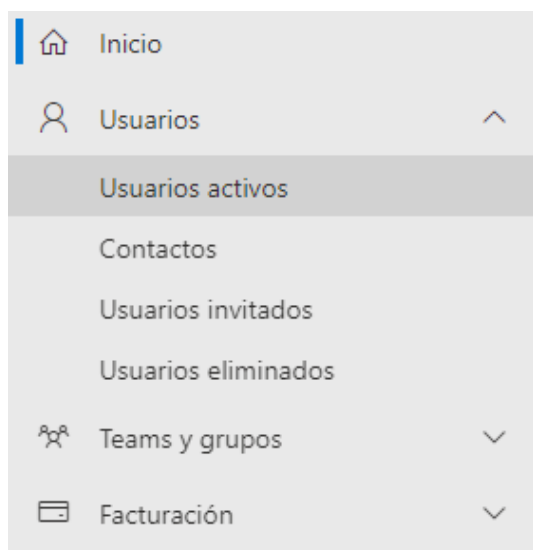
Una vez escaneado el QR nos aparecerá una ventana con un número y automáticamente en la aplicación del móvil nos pedirá que introduzcamos este número.



Al introducir el código en la aplicación del móvil ya tendríamos la verificación doble factor de Microsoft activada.

ILUSTRACIÓN 51: CONFIGURAR DOBLE FACTOR MICROSOFT 3

En este caso, al formar parte de una empresa, una vez hemos realizado estos pasos el administrador de nuestra red, que en este caso soy yo, tendrá que habilitarnos para poder utilizar la verificación de doble factor, si queremos utilizar el doble factor de Microsoft a nivel personal no haría falta habilitar nada.



Para habilitar a los usuarios nos dirigiremos al Centro de administración de Microsoft 365 y en el menú que nos aparece a la izquierda pulsaremos sobre Usuarios y se nos abra un desplegable, en este desplegable pulsaremos sobre Usuarios activos.

Una vez dentro de la ventana de usuarios activos a la parte superior de la ventana tenemos un menú y en este menú tenemos que pulsar sobre Autenticación multifactor.


 Autenticación multifactor

ILUSTRACIÓN 52: HABILITAR USUARIOS 1

Al pulsar sobre Autenticación multifactor se nos abrirá una nueva ventana con el listado de todos los correos electrónicos que hay dentro de la empresa y el estado en el que está.

Arnau Vidal Millan

arnau.vidal@cerdagroup.com

Deshabilitada

ILUSTRACIÓN 53: HABILITAR USUARIO 2

Al pulsar sobre el correo electrónico que queramos habilitar nos aparecerá un menú a la derecha donde nos pondrá en azul “Habilitar”, al pulsar sobre este botón se nos abrirá una ventana donde tendremos que confirmar que queremos habilitar la autenticación multifactor sobre este usuario.

De esta manera ya tendríamos habilitada la autenticación multifactor.

Arnau Vidal Milla

arnau.vidal@cerdagroup.com

quick steps

Habilitar

Administrar configuración de usuario

Arnau Vidal Millan

arnau.vidal@cerdagroup.com

Habilitado

ILUSTRACIÓN 54: HABILITAR USUARIO 3

VPN para teletrabajar

El doble factor de autenticación para la VPN que se utiliza para teletrabajar es un poco diferente al que utilizamos para las cuentas de Microsoft, pero la finalidad es la misma.

Esta verificación funciona con un código que cada treinta segundos se va cambiando, este código lo obtenemos de la aplicación del móvil llamada Google Authenticator.

Cómo configurar la verificación doble factor para la VPN

Lo primero que tenemos que hacer para empezar a configurar la verificación doble factor para la VPN es descargarnos la aplicación de Google authenticator.

Una vez instalada, abrimos la aplicación y accedemos con la opción “Usar Google authenticator sin una cuenta”, aquí dentro pulsaremos sobre el botón que dice “Agregar un código” y esperaremos al siguiente paso para escanear el QR.



ILUSTRACIÓN 55: GOOGLE AUTHENTICATOR LOGO

Ahora desde el navegador del portátil accedemos a la web vpn.cerdagroup.com.

Para acceder a esta web necesitamos estar fuera de la red de la empresa ya que la vamos a usar para la VPN que se utiliza para teletrabajar.

Dentro de esta web necesitaremos iniciar sesión con nuestras credenciales de dominio y nos aparecerá un código QR el cual tendremos que escanear con el móvil.



ILUSTRACIÓN 56: CONFIGURAR VERIFICACIÓN VPN 1

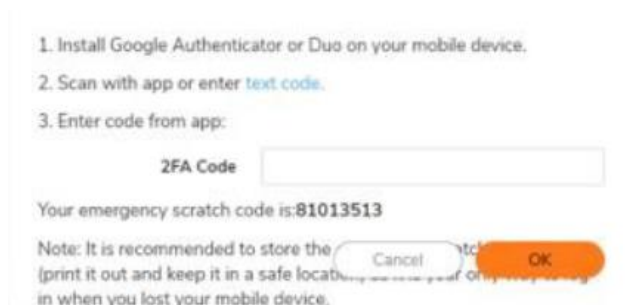


ILUSTRACIÓN 57: CONFIGURAR VERIFICACIÓN VPN 2

Al escanear el código QR en nuestro móvil nos dará un código que tendremos que insertar en el campo donde dice 2FA Code.

Una vez terminados estos pasos ya tendríamos la doble autenticación de la VPN configurada y solo nos quedaría probar a conectarnos.

Demostración del funcionamiento

BitWarden

Para comprobar que Bitwarden funciona correctamente tenemos que dirigirnos a una web donde previamente hayamos guardado un inicio de sesión.

Para comprobar el funcionamiento del gestor de contraseñas decidí guardar mis credenciales de inicio de sesión de la web del centro donde se realizó la propuesta para este proyecto, la web es:

<https://www.ieslluissimarro.org/aplicacions/simjobs/>

Si nos fijamos en el logo de la extensión de Bitwarden aparece un número, este número nos quiere decir que en la página web donde nos encontramos tenemos un inicio de sesión guardado, si nos apareciera un 2 tendríamos dos inicios de sesión diferentes guardados y así sucesivamente.



ILUSTRACIÓN 58:
NUMERO DE INICIOS
DE SESIÓN
GUARDADOS

Algo muy importante de esto es que nos puede ayudar a detectar páginas web que sean falsas y que se utilicen para robar credenciales de inicio de sesión a la gente ya que si nos envían un enlace de una página web donde previamente hemos guardado un inicio de sesión y al entrar a dicha web vemos que el icono de Bitwarden no le aparece el número esto nos indica que esta página web no es la oficial y nuestros datos podrían estar en peligro.

Siguiendo con la demostración, si nos dirigimos a la ventana donde tenemos que poner nuestros datos para iniciar sesión y pulsamos sobre alguno de los campos que tenemos que rellenar el propio Bitwarden nos mostrara un recuadro donde se encuentran guardadas nuestras credenciales.

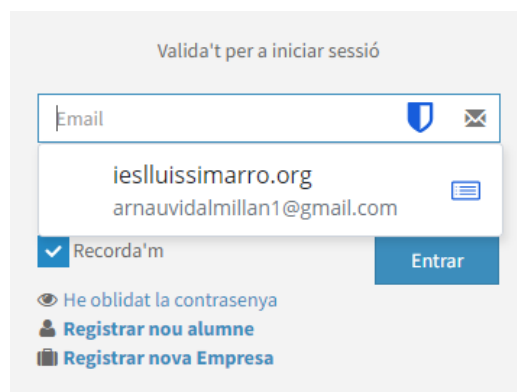


ILUSTRACIÓN 59: FUNCIONAMIENTO BITWARDEN 1

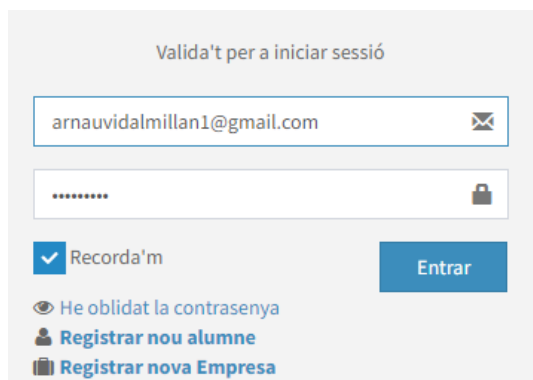


ILUSTRACIÓN 60: FUNCIONAMIENTO BITWARDEN 2

Al pulsar sobre este recuadro los campos se autocompletarán y ya podremos iniciar sesión con normalidad

Doble factor Microsoft

Para comprobar si el doble factor de verificación de Microsoft está funcionando nos dirigiremos a cualquier web donde necesitemos iniciar sesión con nuestra cuenta de Microsoft, en mi caso voy a entrar en la web de office.

Lo primero que tenemos que hacer es cerrar la sesión si ya la teníamos abierta ya que al tenerla ya abierta no nos pedirá nada y nos entrará automáticamente.

Para cerrar sesión nos dirigimos arriba a la derecha, pulsamos sobre nuestro perfil y nos aparecerá la opción para cerrar la sesión.

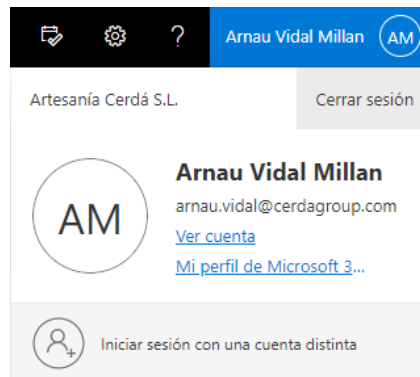


ILUSTRACIÓN 61: CERRAR SESIÓN OFFICE



ILUSTRACIÓN 62: FUNCIONAMIENTO DOBLE FACTOR MICROSOFT 1

Al darle al botón para iniciar sesión nos aparecerá un número de dos dígitos en la pantalla, y a la vez en el móvil nos aparecerá una notificación que nos dice si somos nosotros los que estamos intentando iniciar sesión.

Una vez ya tenemos la sesión cerrada tendremos que volver a iniciar sesión, en mi caso tengo la contraseña guardada en Bitwarden, por tanto, solo tendré que pulsar sobre el recuadro que me aparece al intentar rellenar uno de los campos.

arnau.vidal@cerdagroup.com
Aprobar la solicitud de inicio de sesión

Abra la aplicación Authenticator y escriba el número que se muestra para iniciar sesión.

31

ILUSTRACIÓN 63: FUNCIONAMIENTO DOBLE FACTOR MICROSOFT 2

¿Está intentando iniciar sesión?

Artesanía Cerdá S.L.
arnau.vidal@cerdagroup.com

Escriba el número que se muestra para iniciar sesión.

Escriba el número aquí

SÍ

NO, NO SOY YO

NO PUEDO VER EL NÚMERO

ILUSTRACIÓN 64: FUNCIONAMIENTO DOBLE FACTOR MICROSOFT 3

Al pulsar sobre esta notificación nos aparecerá en el móvil una ventana donde tendremos que introducir este número de dos dígitos.

Al introducirlo pulsaremos sobre el botón que dice Sí y ya nos iniciara sesión con normalidad.

Doble factor VPN

Para comprobar el funcionamiento de la verificación de doble factor para la VPN que utilizan los trabajadores para teletrabajar nos dirigiremos a la aplicación llamada Netextender que es la VPN que se utiliza aquí en Artesanía Cerda S.L.

Al abrir la aplicación tendremos que especificar el servidor al que nos queremos conectar, el usuario con el que queremos conectarnos y el dominio al que pertenecemos.

- Server: vpn.cerdagroup.com
- Username: usuario del dominio
- Password: contraseña del dominio
- Domain: cerdacompany.com

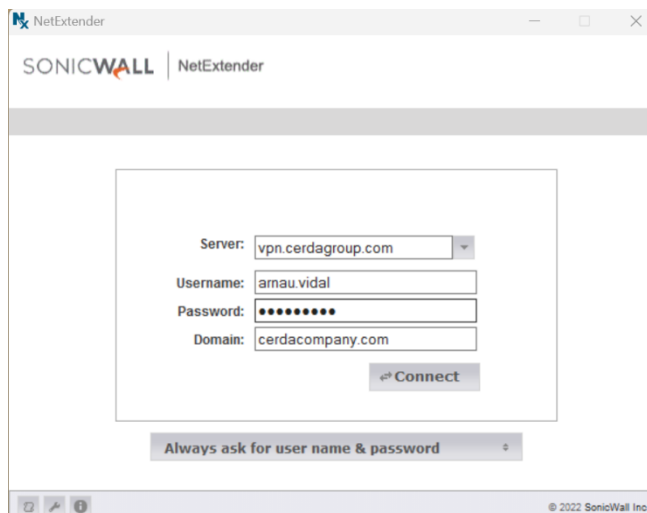


ILUSTRACIÓN 65: FUNCIONAMIENTO DOBLE FACTOR VPN 1

Una vez ya tenemos todos los campos completados pulsaremos sobre el botón que dice “Connect” y nos pedirá que introduzcamos una contraseña, esta contraseña es el código que nos proporciona la aplicación de Google authenticator.

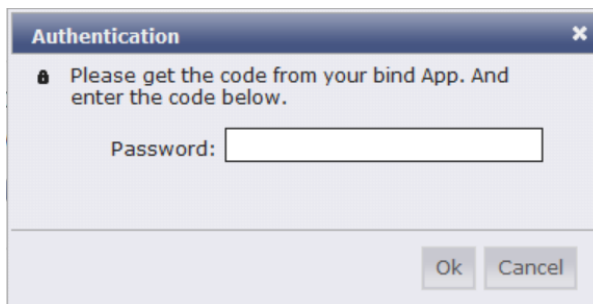


ILUSTRACIÓN 66: FUNCIONAMIENTO DOBLE FACTOR VPN 2

Finalmente, al introducir el código ya estaríamos conectados a la VPN.



ILUSTRACIÓN 67: FUNCIONAMIENTO DOBLE FACTOR VPN 3

Evaluación de los resultados

Una vez finalizado el largo proceso de implementación de todos estos sistemas de seguridad nos hemos podido dar cuenta que la empresa ha mejorado en los siguientes aspectos:

- **Mayor seguridad de las contraseñas**

La implementación de un gestor de contraseñas ha ayudado a los empleados a gestionar sus contraseñas de forma segura y eficiente. Esto reduce el riesgo de que se filtren las contraseñas, fortaleciendo la seguridad de las cuentas y los datos sensibles de la empresa.

- **Protección adicional con la verificación en dos pasos de Microsoft**

La activación de la verificación en dos pasos proporciona una capa adicional de seguridad al requerir un segundo método de autenticación, como un código enviado al teléfono móvil del usuario. Esto hace que sea mucho más difícil para los hackers acceder a las cuentas incluso si obtienen la contraseña.

- **Mayor protección de la red con la verificación en dos pasos para la VPN**

Al implementar la verificación en dos pasos para la VPN que utilizan los empleados para teletrabajar, se asegura que solo los usuarios autorizados puedan acceder a la red corporativa. Esto reduce significativamente el riesgo de accesos no autorizados y protege la integridad de los datos corporativos.

- **Cultura de Seguridad Reforzada**

La introducción de estas medidas de seguridad no solo protege los activos de la empresa, sino que también promueve una cultura de seguridad entre los empleados. Al priorizar la seguridad de la información y proporcionar herramientas para protegerla, estás fomentando prácticas seguras en toda la organización.

- **Reducción del riesgo de brechas de seguridad**

En general, estas medidas combinadas reducen significativamente el riesgo de brechas de seguridad y ataques cibernéticos. Al proteger las contraseñas, los dispositivos y la red, estás fortaleciendo la postura de seguridad de la empresa y mitigando posibles riesgos para la continuidad del negocio.

En resumen, la implementación de un gestor de contraseñas, la verificación en dos pasos de Microsoft y la verificación en dos pasos para la VPN son decisiones positivas que han mejorado la seguridad de la empresa y fortalecido la protección de los datos corporativos, al tiempo que promueven una cultura de seguridad entre los empleados.

En las siguientes capturas se demuestra que todos estos sistemas de seguridad se están utilizando

Bitwarden:

9 may 2024, 12:18:00	Extensión - Chrome		Elemento 817ab47e visto.
9 may 2024, 12:18:00	Extensión - Chrome		Elemento 817ab47e editado.
9 may 2024, 12:17:56	Extensión - Chrome		Contraseña para el elemento 817ab47e vista.
9 may 2024, 12:17:54	Extensión - Chrome		Elemento 817ab47e visto.
9 may 2024, 12:17:41	Extensión - Chrome		Contraseña para el elemento 817ab47e vista.
9 may 2024, 12:17:38	Extensión - Chrome		Elemento 817ab47e visto.
9 may 2024, 12:17:28	Extensión - Chrome		Elemento 817ab47e autorrellenado.
9 may 2024, 12:15:47	Extensión - Chrome		Elemento 817ab47e autorrellenado.
9 may 2024, 12:15:37	Extensión - Chrome		Elemento 817ab47e autorrellenado.
9 may 2024, 10:50:23	Extensión - Chrome		Elemento 95845ba4 autorrellenado.
9 may 2024, 10:50:21	Extensión - Chrome		Elemento 95845ba4 autorrellenado.
9 may 2024, 10:47:54	Extensión - Chrome		Contraseña para el elemento 980579c2 copiada.
9 may 2024, 10:44:54	Extensión - Chrome		Elemento 7bb36d42 autorrellenado.
9 may 2024, 10:26:04	Extensión - Chrome		Elemento 84bae025 autorrellenado.
9 may 2024, 10:26:00	Extensión - Chrome		Elemento 84bae025 autorrellenado.
9 may 2024, 9:19:45	Extensión - Chrome		Elemento 980579c2 autorrellenado.
9 may 2024, 8:43:09	Extensión - Chrome		Elemento 4bce1191 autorrellenado.
9 may 2024, 8:40:49	Extensión - Chrome		Elemento 4bce1191 autorrellenado.
9 may 2024, 8:38:52	Extensión - Chrome	Arnau Vidal	Elemento 4bce1191 autorrellenado.
9 may 2024, 8:20:40	Caja fuerte Web - Chrome	Arnau Vidal	Identificado.
9 may 2024, 8:11:34	Extensión - Chrome		Elemento 80a3e791 autorrellenado.
9 may 2024, 7:22:48	Extensión - Chrome		Elemento 95845ba4 autorrellenado.
9 may 2024, 7:03:54	Extensión - Chrome		Elemento fe7a0fc2 autorrellenado.
9 may 2024, 0:48:56	Extensión - Edge		Elemento 9c29e8ae autorrellenado.

ILUSTRACIÓN 68: REGISTRO DE BITWARDEN

Esta captura de pantalla es un historial de toda la actividad que está teniendo Bitwarden, en concreto el día 9 de mayo desde las 7 de la mañana hasta las 12 de la mañana (solo aparece mi nombre ya que por respeto y petición de la empresa he borrado el de los otros trabajadores).

En la siguiente captura se puede ver una lista donde se muestra que los usuarios están habilitados en el doble factor de autenticación de Microsoft (solo se muestra una pequeña parte de todos los trabajadores que hay ya que hay 98 habilitados).

NOMBRE PARA MOSTRAR	NOMBRE DE USUARIO	ESTADO DE MULTI-FACTOR AUTH
	@cerdagroup.com	Habilitado
	@cerdagroup.com	Habilitado
	@cerdagroup.com	Habilitado
	@cerdagroup.com	Habilitado
	@cerdagroup.com	Habilitado
	@cerdagroup.com	Habilitado
	@cerdagroup.com	Habilitado
	@cerdagroup.com	Habilitado
Arnau Vidal Millan	arnau.vidal@cerdagroup.com	Habilitado
	@cerdagroup.com	Habilitado
	@cerdagroup.com	Habilitado
	@cerdagroup.com	Habilitado
	@cerdagroup.com	Habilitado
	@cerdagroup.com	Habilitado
	@cerdagroup.com	Habilitado
	@cerdagroup.com	Habilitado
	@cerdagroup.com	Habilitado
	@cerdagroup.com	Habilitado
	@cerdagroup.com	Habilitado

ILUSTRACIÓN 69: USUARIOS HABILITADOS

Con la VPN no hay un registro igual que con la verificación de Microsoft o con Bitwarden pero todos los trabajadores tienen puesto el autenticador ya que sin esta no podrían teletrabajar.

Conclusiones

Los resultados obtenidos con el desarrollo de este proyecto han sido bastante buenos ya que se han cumplido satisfactoriamente todos los objetivos planteados inicialmente.

Ha sido un proceso largo ya que teníamos que explicar de uno en uno a todos los empleados de la empresa todas las mejoras de seguridad que se iban a implementar para así asegurarnos de que las utilizaran de una forma correcta, el proceso duró un mes y medio, desde el 25/03/2024 hasta el 10/05/2024.

Me gustaría decir que este proyecto ha supuesto una evolución en mi forma de ver la seguridad en la informática, después de este mes y medio implementando los servicios me he dado cuenta de lo fácil que es para un hacker obtener una contraseña, también me he dado cuenta de que no sirve con tener una simple contraseña y utilizarla para todas las páginas donde nos registramos porque de esta manera van a tener acceso a todos nuestros datos.

Personalmente voy a empezar a utilizar Bitwarden y la verificación doble factor de Microsoft, también voy a modificar mis contraseñas para cumplir con los requisitos que hemos especificado anteriormente, de esta manera mis contraseñas serán más difíciles de descifrar, estarán guardadas en un sitio seguro y si por alguna razón consiguieran mis contraseñas para iniciar sesión, en Microsoft tendría la doble verificación activada y los atacantes no podrían acceder a mis datos.

Finalmente me gustaría decir que técnicamente puede que no sea el mejor proyecto del mundo, pero personalmente puedo decir que ha sido un proceso bastante interesante el hecho de haber implementado estos sistemas de seguridad a toda una empresa y creo que es algo bastante útil tanto para otras organizaciones como para el uso personal.

Recursos utilizados

Los recursos que se han utilizado durante este proyecto son los siguientes:

Hardware

- Portátil Lenovo Thinkpad Intel i5-1035G1, 8GB RAM, 256GB SSD donde se ha configurado todo
- Móvil propio para los autenticadores
- Cada trabajador ha utilizado su portátil para tener el gestor de contraseñas
- Cada trabajador ha utilizado su móvil para tener los autenticadores

Software

- Servicio que nos ofrece Bitwarden
- Aplicación Google Authenticator
- Aplicación Microsoft Authenticator

Tabla de ilustraciones

Ilustración 1: Actividades sospechosas que detecta el firewall	5
Ilustración 2: Correo que envía el atacante	6
Ilustración 3: Logo bitwarden	8
Ilustración 4: Nube encriptada.....	8
Ilustración 5: Comparación Bitwarden y Google	11
Ilustración 6: Crear carpetas 1	15
Ilustración 7: Crear carpetas 2	15
Ilustración 8: Carpetas creadas 1	15
Ilustración 9: Carpetas creadas 2	16
Ilustración 10: Carpetas creadas 3	16
Ilustración 11: Carpetas creadas 4	16
Ilustración 12: Carpetas creadas 5	16
Ilustración 13: Crear grupos 1	17
Ilustración 14: Crear grupos 2	17
Ilustración 15: Crear grupos 3	18
Ilustración 16: Grupos creados	18
Ilustración 17: Permisos Logistics.....	19
Ilustración 18: Permisos Supply Chain	19
Ilustración 19: Permisos Production & Purchasing	19
Ilustración 20: políticas 1	20
Ilustración 21: políticas 2	20
Ilustración 22: Política contraseñas	20
Ilustración 23: Política recuperar cuenta 1	20
Ilustración 24: Política recuperación cuenta 2.....	21
Ilustración 25: Política recuperación cuenta 3.....	21
Ilustración 26: Política generador de contraseñas	22
Ilustración 27: Política organización única	22
Ilustración 28: Invitar usuarios 1	23
Ilustración 29: Invitar usuarios 2	23
Ilustración 30: Correo de invitación	24
Ilustración 31: Crear cuenta en bitwarden	25
Ilustración 32: Iniciar sesión en bitwarden.....	25
Ilustración 33: Aceptar usuarios en bitwarden	26
Ilustración 34: Caja fuerte	26
Ilustración 35: Agregar extensión 1.....	27
Ilustración 36: Agregar extensión 2.....	27
Ilustración 37: Agregar extensión 3.....	27
Ilustración 38: Agregar extensión 4.....	28
Ilustración 39: Agregar contraseña de forma manual.....	29

Ilustración 40: Agregar contraseña de forma automática.....	30
Ilustración 41: Agregar contraseñas importándolas 1	30
Ilustración 42: Agregar contraseñas importándolas 2	30
Ilustración 43: Agregar contraseñas importándolas 3	31
Ilustración 44: Compartir contraseña 1	31
Ilustración 45: Compartir contraseña 2	32
Ilustración 46: Usuarios dentro de la organización	32
Ilustración 47: Verificación doble factor	33
Ilustración 48: Logo aplicacion Microsoft authenticator	34
Ilustración 49: Configurar doble factor Microsoft 1	34
Ilustración 50: Configurar doble factor Microsoft 2	34
Ilustración 51: Configurar doble factor Microsoft 3	35
Ilustración 52: Habilitar usuarios 1	35
Ilustración 53: Habilitar usuario 2	35
Ilustración 54: Habilitar usuario 3	36
Ilustración 55: Google authenticator logo	36
Ilustración 56: Configurar verificación VPN 1	37
Ilustración 57: Configurar verificación VPN 2	37
Ilustración 58: Numero de inicios de sesión guardados	38
Ilustración 59: Funcionamiento bitwarden 1	38
Ilustración 60: Funcionamiento bitwarden 2	38
Ilustración 61: Cerrar sesión office	39
Ilustración 62: Funcionamiento doble factor microsoft 1	39
Ilustración 63: Funcionamiento doble factor Microsoft 2	39
Ilustración 64: Funcionamiento doble factor Microsoft 3	39
Ilustración 65: Funcionamiento doble factor VPN 1	40
Ilustración 66: Funcionamiento doble factor VPN 2.....	40
Ilustración 67: Funcionamiento doble factor VPN 3.....	40
Ilustración 68: Registro de Bitwarden	42
Ilustración 69: Usuarios habilitados	43

Bibliografía

Página web de Bitwarden

<https://bitwarden.com/es-la/>

Wikipedia sobre Bitwarden

<https://es.wikipedia.org/wiki/Bitwarden>

Precios de Bitwarden

<https://bitwarden.com/es-la/pricing/>

Diferencias de Bitwarden y Chrome

<https://otroconcepto.com/protege-tus-contrasenas-chrome-vs-bitwarden-una-comparativa-detallada/>

Información sobre la verificación en dos pasos de Microsoft

<https://support.microsoft.com/es-es/account-billing/c%C3%B3mo-utilizar-la-verificaci%C3%B3n-en-dos-pasos-con-su-cuenta-de-microsoft-c7910146-672f-01e9-50a0-93b4585e7eb4>

Wikipedia sobre la aplicación de Google Authenticator

https://es.wikipedia.org/wiki/Google_Authenticator

Anexos

Repositorio GitHub: <https://github.com/Arni72/TFG>

En este repositorio de GitHub encontraras todos los archivos que se han utilizado para este proyecto.

Contenido del repositorio:

- Memoria del proyecto
- Presentación del proyecto
- Todas las imágenes utilizadas en la memoria
- Resumen de una hoja sobre la memoria
- Video donde se explica a un trabajador como implementar el nuevo gestor de contraseñas y cómo funciona
- Archivos para trabajadores

Dentro de la carpeta Archivos para trabajadores se puede encontrar toda la información que se les envió a los trabajadores de la empresa durante el tiempo que duro el proceso de implementación de los sistemas de seguridad.

Contenido:

- Bitwarden.pdf: este PDF contiene información sobre el gestor de contraseñas que se iba a implementar.
- Formación Phishing.pptx: al no saber cómo consiguieron el acceso al correo del trabajador se hizo un PowerPoint donde se explica que es la ciberseguridad y como identificar un correo malicioso.
- Verificación doble factor Microsoft.pdf: este PDF contiene información sobre la verificación doble factor de Microsoft.
- Verificación doble factor VPN.pdf: este PDF contiene información sobre la verificación doble factor para la VPN.