CIBERSEGURIDAD ATALAYA

Todo lo que necesitas saber, en un solo manual

Nuestro **objetivo** es concienciar y enseñar cómo **protegerte** de los **riesgos** digitales como usuario en dispositivos electrónicos

01 Ciberseguridad en Nuestro Equipo

02 Ciberseguridad en Nuestro Mail

03 Ciberseguridad Web

04 Ciberseguridad en la Red

05 Antivirus + Firewall

06 Información Confidencial

07 Protocolo Gestión de Incidentes

¡Lectura rápida, útil y esencial para todos!

Descubre más

CIBERSEGURIDAD EN NUESTRO EQUIPO

Los dispositivos que utilizamos en el entorno laboral deben mantenerse **seguros** mediante **buenas prácticas** y **herramientas adecuadas**

Servicios Corporativos Asociados

- **Trendmicro** (Antivirus y Antispam)
- **Sharepoint** (Ficheros compartidos)
- **Fortinet** (Firewall)
- **Darktrace** (Tráfico de red)
- **Bullwall** (Anti-encriptación)

Conciencia sobre Amenazas

- Evita compartir credenciales por medios inseguros
- Mantén buenas prácticas de seguridad
- Protege tu cuenta corporativa

ⓘ Sé parte activa de la Seguridad

CIBERSEGURIDAD EN NUESTRO MAIL

El **correo electrónico** es una herramienta esencial, pero también un canal común para intentos de **engaño (phishing)**

Recomendaciones Básicas

NO ABRAS
correos de remitentes desconocidos

DESCONFÍA
de mensajes urgentes

EVITA
hacer clic en enlaces sospechosos

NUNCA
compartas información confidencial

VERIFICA
el remitente y que el email esté bien escrito

INFORMA
a IT si recibes un correo sospechoso

ⓘ ¿Dudas con un correo? Contacta a IT

CIBERSEGURIDAD WEB

Navegar por **internet** es parte del trabajo diario, pero también un **riesgo** si no se toman precauciones

Peligros Frecuentes

- Enlaces maliciosos y sitios falsos
- Uso de software no autorizado
- Phishing y suplantaciones
- Almacenamiento en la nube no corporativo

Buenas Prácticas

- Verifica sitios web
- Evita el uso de servicios online no autorizados
- No uses software pirata o crackeado
- No uses cuentas personales en la nube
- Cuidado con servicios online gratuitos
- Detecta el phishing y spoofing

ⓘ Recuerda: la Seguridad empieza contigo

CIBERSEGURIDAD EN LA RED

Conectarte a **redes WiFi inseguras** puede poner en **riesgo** tu información. Sigue estos consejos y **protégete** al usar Internet

Evita redes WiFi públicas

- **No uses WiFi gratuito** (aeropuertos, cafés, hoteles o centros comerciales)
- Son redes **no seguras**

Recomendaciones Clave

- Usa redes conocidas y **protegidas con contraseña** (como la de nuestra oficina)
- **No ingreses datos sensibles** desde redes públicas (contraseñas, bancarios o corporativos)
- **Fuera de casa** usa datos móviles o una VPN aprobada por tu empresa
- **Verifica el nombre legítimo** de la red antes de conectarte

Cuidado con Ataques Man-in-the-Middle

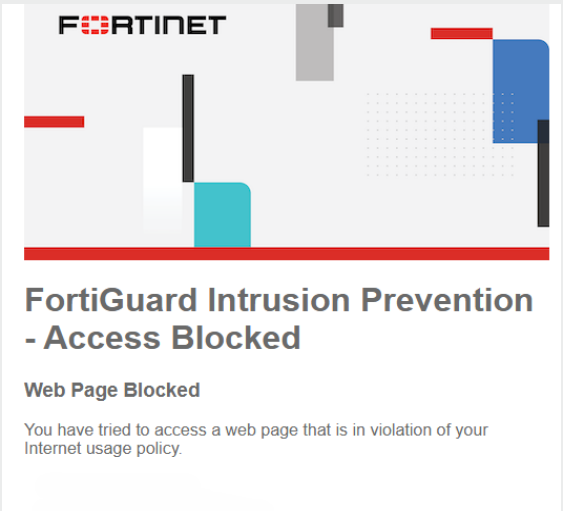
- Un atacante puede **clonar** una red WiFi y engañar a tu dispositivo
- Si te conectas a esa red falsa, tu información puede ser **interceptada**

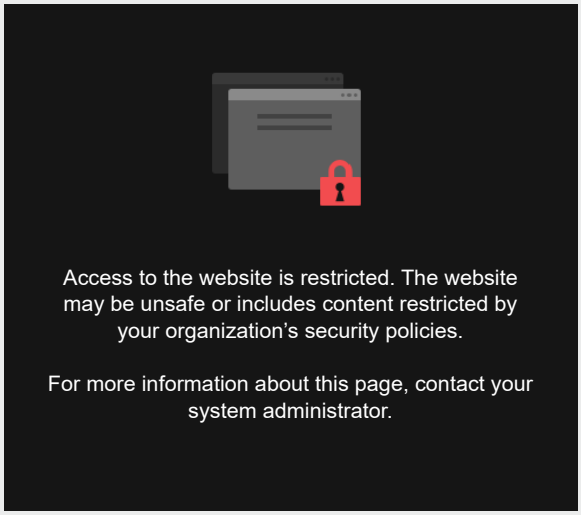
ⓘ Mantén precauciones y protégete

ANTIVIRUS + FIREWALL

Todos los equipos de la empresa se encuentran tras un **Firewall Corporativo Perimetral**, y están protegidos con un **Antivirus + Antispam** que actúan automáticamente. Si aparece un mensaje de **advertencia**, no es un error: es el sistema trabajando para **bloquear** amenazas y **proteger** tanto tu información como la de la empresa

Mensajes de Advertencia





¿Qué debe hacer el Usuario?

- No alarmarse. Es una medida preventiva
- No forzar el acceso
- Cerrar la página o cancelar la descarga inmediatamente
- En caso de que el bloqueo afecte una página o archivo que necesites, contactar con el Departamento de IT

INFORMACIÓN CONFIDENCIAL

¿Qué se considera Confidencial?

- Datos de clientes, proveedores o empleados
- Documentos internos, presupuestos, reportes, estrategias...
- Accesos, contraseñas o credenciales de sistemas
- Conversaciones internas no pensadas para compartirse fuera

Recomendaciones Básicas

- No enviar **documentos sensibles** por canales **no autorizados**
- **No compartir** pantallazos, fotos o comentarios sobre el trabajo en redes sociales
- No hablar de **temas confidenciales** en lugares públicos o con personas ajenas a la empresa
- Guardar siempre los **archivos importantes** en los servidores de la empresa, nunca en equipos personales

Si no estás seguro de algo, consulta con tu responsable de departamento, con el equipo de Legal o con el equipo de IT

PROTOCOLO GESTIÓN INCIDENTES

Tan importante es **prevenir** los incidentes relacionados con la ciberseguridad como **actuar rápidamente** cuando se detecte uno

¿Qué se considera un Incidente de Seguridad?

- Recibir un correo que parece fraudulento o con enlaces sospechosos y pulsar en alguno de los enlaces
- Descargar o abrir un archivo que genera errores
- Detectar que el equipo va más lento de lo normal después de haber entrado en algún enlace o App sospechosa
- Perder o que te roben un dispositivo con acceso a información de la empresa
- Sospechar que alguien no autorizado accedió a un sistema o a una cuenta
- Poner tu usuario/contraseña en un sitio sospechoso

¿Qué hacer ante un Incidente?

- No ignores el problema
- Informa de inmediato al área de Tecnología o al contacto de soporte
- Abrir un ticket de soporte en IT
- Siempre en caso de duda, comentarlo con algún compañero del área de Ciberseguridad de IT