Osix

Corporation

Seguridad en Osix

Director Eduard Castelló

Encargado Alejandro berenjena

Diseñador Eduard Castelló

Participantes Fernando roure

Sergi palacios

2020

Introducción

Este documento pretende contener toda la información necesaria tanto para la ciberseguridad de la empresa como para la de sus empleados, distribuidores y clientes, de esta forma, podremos ver qué directrices va a seguir la empresa para hacer posible la mejor seguridad actual, disponiendo de un itinerario donde vamos a ver los pasos que seguirá nuestra empresa, continuando con las descripciones de los trípticos y demás informaciones y finalmente detallando los protocolos que seguirá Osix, detallados y con la información concisa para que todo empleado o cliente pueda entender porque es segura nuestra empresa y que hacemos dia a dia para que lo siga siendo.

Itinerario Osix

En nuestro itinerario lo principal que tenemos en cuenta es la seguridad de los datos que manejamos, ya que nuestra empresa controla datos tanto personales como bancarios y o influyentes para a nuestros clientes, tal es así que una pérdida ínfima de estos podría causar el cierre de nuestra empresa.

Una vez esta idea está clara empezaremos a explicaros los puntos de dicho itinerario y todo aquello que seguimos para llegar a lo recién explicado.

Riesgos del sector

1. Pérdida de datos personales y bancarios
2. Fraude online
3. Sistemas desactualizados y vulnerables
4. Cese de actividad
5. Sanción por incumplimiento legal

Estos 5 apartados son los riesgos de nuestra empresa todos ellos supondría una misma cosa pérdidas para nuestra empresa y de un modo u otro un peligro para la continuidad de la misma.

La mayoría de estos riesgos se basan en los datos y la usurpación de estos, por eso explicamos su importancia previamente por que en un sistema como el nuestro es lo que más se valora, ya que, si robas una cuenta bancaria que estaría situada en el primer punto también se verían involucrados el punto 2, 4 y 5 podría ser el 3 también, pero nos tendríamos que cerciorarse por que el fallo de seguridad podría deberse a sistema desactualizado o no simplemente que un ciberdelincuente haya sobrepasado el sistema.

Los enemigos de la empresa

Muchas veces los enemigos de nuestra empresa son de esta misma, sean directos o no muchas veces los propios empleados causan estragos en la empresa, ya sea tocando algo que no deben y eliminando datos existenciales de la misma o ex empleados que aún conserven acceso a la empresa y maliciosamente extraigan información de esta para venderla y perjudicar a la empresa.

Por otra parte, también es evidente que hay ciberdelincuentes que buscan robar a la empresa para su beneficio propio y hay que tenerlos en cuenta.

Otro apartado sería nuestra propia seguridad nos podría dar una falsa seguridad ya sea por fallos del sistema o por su falta de configuración.

Por otra parte, podría haber intervenido un virus y facilitar así la entrada de un ciberdelincuente.

Como otro enemigo clave encontramos a la competencia del sector en el que trabajamos, que para facilitar su propio crecimiento hunde otras empresas de sus alrededores.

Plan Director de Seguridad

Debemos analizar con claridad nuestra empresa y llevar a cabo un determinado análisis de seguridad para determinar qué nivel de seguridad queremos y necesitamos en nuestra empresa

Deberemos también definir los proyectos de la empresa para saber cómo estructuran el plan.

Hacer una clasificación y priorización de datos más valiosos y los cuales deben estar más o menos seguros.

Lo pasamos a dirección para que sea aprobado y lo aplicamos para estructurar toda la información.

De todas formas, nunca se puede estar tranquilo antes estos ataques, pero todo esto es un ejemplo de mejora continua así que avanzaremos progresivamente y podremos estar algo más aliviados.

Puesto de trabajo

Hay que cuidar siempre nuestro puesto de trabajo, esto significa nada de contraseñas en post-its, papeles confidenciales bien guardados y si es bajo llave mejor, papeles confidenciales que ya no sean importantes destruirlos en la trituradora siempre ya que esa información sigue siendo confidencial.

Todo esto es muy importante ya que un pequeño fallo en nuestro puesto de trabajo supondría una falla grande de seguridad en nuestra empresa.

Fuera de la oficina

Fuera de la oficina tampoco debemos bajar la guardia, ya que nos rodea mucha gente y nunca podemos saber lo que esa gente piensa así que, si nos descuidamos de nuestro ordenador o tenemos una conversación confidencial podría haber gente husmeando la cual podría intervenir en la seguridad de la empresa, así que nunca bajéis la guarda ya que podría suponer un error muy grande.

Emails sospechosos

Al trabajar con correos es fácil recibir correos engañosos los cuales se utilizan para el robo de contraseñas para poder acceder dentro de la empresa.

Para esto existen diferentes modos uno por ejemplo es el phishing que en lo que se basa es en hacerse pasar por otra persona para realizar un engaño y así conseguir información valiosa.

Otra herramienta sería el spam el cual es un cúmulo de correos no deseados que la mayoría de veces se basan en publicidad no solicitada, pero un pequeño porcentaje es publicidad engañosa la cual solicita nuestra atención para engañarnos y recaudar dinero. Por ello es muy importante saber distinguir los correos y aprender a desechar los correos como estos.

Por último, pero no menos importante encontramos los correos con archivos adjuntos, estos pueden contener malware que puede afectar seriamente a tu ordenador haciéndole perder información valiosa y haciendo gastar un dinero a la empresa para solucionar este virus.

Estos correos suelen ser fáciles de detectar y se suelen asociar al spam así que como dijimos hay que saberlos distinguir bien, por lo tanto, no te descargues nunca un archivo sin antes cerciorarte bien de que es seguro.

Cultura de seguridad

Como vengo explicando la ciberseguridad lo es todo en nuestra empresa, así que culturizarse en seguridad nunca está de más, por lo tanto, hay que tomar conciencia de que la información que almacena la empresa es esencial protegerla.

Además, si seguimos todos los pasos bien y si encontramos problemas los reportamos debidamente con el paso del tiempo crearemos una buena cultura de ciberseguridad.

Pero eso sí para crear una buena cultura de ciberseguridad tenemos que colaborar todos, no penséis que es cosa solo de informáticos, todos aquellos que estemos en la empresa debemos colaborar y aportar nuestro grano de arena.

Recursos Humanos

Para todos aquellos que entren en nuestra empresa les debemos garantizar la información necesaria para que se percatan de la ciberseguridad sea cual sea su sector de trabajo ya que todos importamos por igual cuando hablamos de la ciberseguridad.

Después de esto les debemos asignar los permisos suficientes para la buena realización del trabajo. Pero solo para eso otra información de rango superior no se le otorgara.

También contamos con el proceso de contratación que suele ser el mejor para dotar de conocimientos de ciberseguridad y saber el nivel de recepción que tiene nuestro futuro empleado para ello.

También debemos garantizar una seriedad y firmeza ante esto, ya que es muy importante la sensación que le otorgamos al nuevo empleado para que vea el nivel de importancia de las cosas.

Por último, pero no menos importante es necesario firmar un acuerdo de confidencialidad para que todo lo que le enseñemos no sea filtrado.

En caso de la finalización de un empleado debemos controlar la información que puede llegar a filtrar o en casos extremos la difamación que podría hacer de nuestra empresa.

Para ello debemos despojarle de todos sus accesos a nuestra empresa.

Aunque dudamos que nuestros empleados puedan hacer tales cosas ya que se les instruirá en base del compañerismo. Por lo tanto, serán bien tratados.

Información y su destino

Todo personal nuevo que no sepa dónde ni cómo nos organizamos merece una explicación así que les comunicaremos nuestro PDS para que sepa cómo funcionamos donde almacenamos nuestra información y la gran seguridad que tiene que tener con todos nuestros datos, ya que le debemos transmitir nuestra preocupación por la seguridad.

Con ello le explicaremos a qué información puede acceder y a cuál no ya que dependiendo de su rango de trabajo tendrá una u otra información así también comprenda mejor la importancia de todo esto.

Subcontratación TIC

Dejando a un lado a que compañía subcontratamos tenemos que tener en cuenta que programas y que equipos se nos da, ya que pueden ser correctos o no.

Además, debemos cerciorarnos que nuestra información está siendo almacenada y administrada de la mejor manera posible ya que a parte de la seguridad que tengamos nosotros en nuestra propia empresa debemos intentar controlar que la información que por subcontratación se protege esté bien protegida y segura.

Todo esto debe estar en el contrato de subcontratación para que esté correcto.

Gracias a esto debemos analizar con certeza todo lo que nos ofrecen y realizar un contrato con demandas por fallas y firmar acuerdos de confidencialidad.

Confianza en subcontrataciones TIC

Al fin y al cabo, lo más importante es la confianza que te transmiten ya que si no te transmiten confianza a ti los ciberdelincuentes no tendrán miedo de asaltar tu compañía porque ellos notarán que esa compañía no transmite seguridad y aunque sea más segura tendrán más intentos de asaltos simplemente por ese sentimiento.

Ya que si tú no te sientes seguro es por algo, aparte puedes llegar a acuerdos con la misma compañía y modificar cosas del contrato para sentirte mejor.

Incluso una mejora de productos o un incremento de programas de seguridad.

Nuestra web

¿Nuestra propia web transmite la confianza tan anhelada por nosotros mismos?

Si no es así no esperemos que nadie confié en nosotros ya que si nosotros no confiamos en compañías que no demuestren su seguridad no podemos pretender que los demás lo hagan con nosotros, así que una cosa primordial es transmitir esa confianza que sabemos que tenemos, con una buena página web y comunicando en esta misma toda la seguridad que garantizamos y tenemos para otorgar.

Super contraseñas

Uno de los factores clave para la protección de datos es nuestras contraseñas y qué mejor que aplicar super contraseñas, contraseñas que sean super seguras, así podremos evitar muchos problemas de seguridad en un futuro y nivelar el nivel de seguridad de nuestros datos, aunque lo que también se puede hacer y es incluso mejor es utilizar siempre super contraseñas para que sea incluso más difícil acceder a cualquier dato de nuestra empresa eso sí tendríamos que tener una gran precaución con todos aquellos que obtengan estas super contraseñas ya que podrías dejar de ser super contraseñas.

Trabajo desde el móvil

Si emprendemos nuestro trabajo desde nuestro móvil debemos saber que es lo mismo que un ordenador, debemos estar atentos, ante todo.

Ya que cualquier cosa que instalemos puede ser dañina para el móvil o pedir demasiados permisos para el móvil para así robarnos información, trabajes por donde trabajes nunca debes descuidar tu información confidencial ya que te puede afectar directamente o incluso a la empresa presta atención a los mensajes y a las instalaciones.

Los datos y la ley

Todos debemos saber que nuestros datos están amparados por la ley, así que si recibimos correos los cuales no queremos o publicidad engañosa siempre podremos denunciar al remitente de dicho correo ya que la LOPD ampara nuestra privacidad y los datos que le acompañan por eso es muy importante estar informado de nuestros derechos ante estos mensajes, además si aún y habiendo solicitado la denegación de dichos mensajes.

Pérdida de archivos

Cuando se pierde un archivo se puede intentar recuperar ya que hay aplicaciones para ello, pero hay una falla de seguridad porque hay un archivo que puede interferir en el bienestar de la empresa, ya que puede utilizarse para dañar a la empresa o vender su información.

De todas formas, puedes tener una empresa contratada de soporte informático para facilitar todos estos problemas.

Así puedes tener mayor seguridad y solucionar los problemas de manera más eficiente y segura, así también transmitiremos mayor seguridad.

Aplicaciones Seguras

Para la utilización de aplicaciones seguras siempre nos podemos cerciorar de su seguridad buscando información o contratando a profesionales del tema para que no guíen para la utilización de diferentes aplicaciones, ya que cada aplicación es un mundo, el cual tiene sus pros y sus contras ya que la mayoría de aplicaciones gratuitas suelen cobrarte con tu información y eso es lo primero que no queremos

así que más vale contratar aplicaciones aunque nos cueste dinero antes que dejar nuestros datos en manos ajenas .

Las redes sociales

Las redes sociales son un arma de doble filo, ya que son muy útiles para expandirse y darse a conocer, pero esto hace que sea más fácil la denigración de nuestra empresa y la malversación de la información que publicamos por nuestras redes, ya que vivimos en la época en la cual todo se puede manipular y malinterpretar.

Así que hay que tener mucha precaución por que puede ser muy buen instrumento para la expansión, pero si cometemos un error es el doble de importante que un error normal ya que es mucho más mediático e impactante ya que las redes sociales abren la puerta a convertirte en una empresa mundana sin serlo realmente así que es un adminículo muy útil, pero a la vez muy peligroso.

Hay que cerciorarse si es rentable tener o no, aunque cada vez más es difícil crecer sin redes en este mundo.

También hay que tener en cuenta en las redes sociales de los empleados ya que puedes dar información sin que ellos se den cuenta así que por ética y seguridad habría que poner normas sobre las redes sociales en nuestra empresa, pero eso ya dependerá de la utilización de ellas.

Engaños

Igual que con los correos es necesario cerciorarse con quien estamos hablando ya que pueden hacer suplantación de identidad para conseguir lo mismo de siempre por eso antes de decir nada confidencial asegúrate con quien hablas.

Porque no solo intentan robar información vía pc, sino que todos los métodos de comunicación son los que atacan así que infórmate y asegúrate.

Plan de contingencia

El plan de contingencia es siempre esencial para que toda empresa siga funcionando y es que sin él todo sería un desastre.

Cuando un error aparece debemos tener claro lo que seguir por eso el plan de contingencia siempre tiene que estar actualizado y a la mano de los trabajadores porque nunca se sabe cuándo puede fallar algo.

Para ello debemos conocer muy bien nuestra empresa y saber cómo actuar, ya tenemos cosas que nos pueden ayudar como el PDS que nos puede ayudar a

identificar donde están las cosas y qué cosas son más importantes que otras para continuar su funcionamiento.

Información portátil

Tienes que saber que la información que almacenes en pendrives o discos duros es la más sensible ya que a no ser que pongas clave a dicho aparato si pierdes el aparato pierdes toda su información así que estamos hablando de una información muy sensible que nunca está de más hacer copias y suministrar lo mejor posible también es muy recomendable que crees una contraseña para acceder a dicho aparato.

Información en el aire

Toda la información que compartes vía internet está en el aire por ondas las cuales se pueden detectar y interferir así construyendo una red falsa para robar información muy útil, esto puede pasar conectándose en una wifi que no conoces o directamente en la tuya propia que no sea suficientemente segura así que estate atento a donde te conectas y de quien te fías

Clasifica, Utiliza y Destruye

Una buena forma de no tener problemas es estar bien organizado, así que clasifica tu información, para saber lo más primordial y de qué ámbito es cada cosa.

Utiliza hasta que te sirva la información y una vez te deje de servir destrúyela para que no se filtre y así conseguirás una buena organización y seguridad.

Todos somos seguridad

Por último, conciénciate con todo lo que leíste en que la seguridad de la información es la clave de nuestra era.

Ya que todos nuestros actos en la empresa y fuera de ella pueden afectar directa o indirectamente a esta misma, así que todos somos la seguridad de todos y la de nosotros mismo

Concienciación para fomentar los buenos hábitos de seguridad

Incidentes de seguridad

Es importante mantener la información a buen recaudo, puesto que la falta de disponibilidad, difusión o alteración de esta puede acarrear problemas con el desarrollo de la empresa. Existen tres tipos de incidentes de seguridad que afectan a la información de nuestra empresa:
Accidentales: no intencionados. Borrar accidentalmente un archivo, averías, incendios, etc.
Intencionados por insiders: los insiders son empleados que en ocasiones deciden llevarse información de la empresa
Causados por ciberdelincuentes: estos individuos utilizan malware que introducen aprovechando debilidades en nuestros sistemas

Los tres pilares de la seguridad

En cuanto a la seguridad de la información de nuestra empresa, es importante mantener tres propiedades básicas: disponibilidad, integridad y confidencialidad, eso significa que la información debe estar lista para su uso en cualquier momento, debe estar limpia de fallos y errores y no debe revelarse a individuos o entidades no autorizadas.
Así mismo, es importante la protección de los datos personales, que son todos aquellos datos que contengan información concerniente a personas físicas identificadas o identificables, en otras palabras, debe estar protegida toda aquella información que pueda llevar a conocer a una persona. Debe saberse que llevar a cabo una mala gestión de la información en una empresa que trata con información personal puede suponer graves consecuencias para una empresa así como con su continuidad, para evitarlo, deberemos identificar si se trata con datos especialmente protegidos o a gran escala, y en caso contrario justificarlo debidamente. También debemos garantizar la absoluta confidencialidad, integridad y disponibilidad de los datos personales, garantizar los derechos y libertades a aquellas personas cuya información está bajo custodia de la empresa, para ello; deberán estar informadas de forma visible, accesible, sencilla y transparente, es decir, no se realizará ninguna gestión ni cambio con su información sin que ellos sean notificados; se debe obtener el consentimiento inequívoco para el uso de sus datos; Permite que puedan ejercer sus derechos

«acceso, rectificación, supresión, limitación, portabilidad, oposición y derecho a no ser objeto de decisiones individualizadas e informarles en caso de violaciones de seguridad, y por último permitir que las autoridades verifiquen que el trato de información se realiza correctamente.

Clasificación de la información

Se debe mantener siempre una correcta organización de la información, tanto en formato físico como digital, además es recomendable catalogar otras características como los departamentos que intervienen o ubicación por ejemplo.
Cada empresa debe tener una jerarquía de niveles en función de cuán importante es la confidencialidad de estos, como orientación podríamos tener los siguientes niveles:
confidencial: la confidencialidad de esta información es de vital importancia para el futuro de la empresa
restringida: uso exclusivo para aquellos miembros de la empresa cuyo trabajo no pueda llevarse a cabo sin esa información
de uso interno: uso exclusivo para el personal de la empresa
pública: información que puede ser difundida sin ningún tipo de reparo(contenido publicitario)

Tratamiento de la información

Para proteger la información se llevarán a cabo una serie de controles de seguridad: acceso limitado, cifrado, copias de seguridad, y tratamientos específicos según lo dictado por ley y aquellos sujetos a acuerdos de confidencialidad.
En el cifrado debe escogerse una clave lo más robusta posible, junto con un algoritmo criptográfico fuerte(es preferible que sea de dominio público) deben realizarse comprobaciones periódicas para verificar que el algoritmo no es vulnerable, la pérdida de la clave de descifrado imposibilita el acceso a la información, que debe estar almacenada a buen recaudo, y la herramienta de cifrado debe estar siempre actualizada.
También hay que saber eliminar los metadatos antes de publicar o enviar cualquier archivo, ya que pueden contener información valiosa para los ciberdelincuentes. Aunque la mayoría de aplicaciones ofimáticas contienen herramientas para este fin, a través de windows también podemos hacerlo.

Copias de seguridad

Otra tarea a llevar a cabo es realizar copias de seguridad de nuestra información, ya que de no hacerlo, podrían sufrirse graves consecuencias, para evitarlo, debemos volver a la clasificación de antes, en función de ella se identificarán y copiaran aquellos datos cruciales para que la empresa pueda seguir con su actividad diaria. Es importante definir una adecuada frecuencia de la realización de estas copias, de manera que no suponga una gran pérdida, ni afecte negativamente en la actividad laboral. Existen diferentes tipos de copias de seguridad:
El Raid 1 mediante el cual se crean se crea una copia exacta en tiempo real con la que se evita guardar datos obsoletos, la principal desventaja es que si este sistema sufre un fallo, hackeo o modificación

Tipos de copias de seguridad

completa: consiste en hacer una copia de todos los datos de nuestro sistema en otro soporte haciendo que la recuperación,en caso de incidente, sea mucho más rápida. Pero requiere de un mayor tiempo para realizar la copia y mayor coste económico.
diferencial: únicamente se copian los archivos y directorios que han sido creados o modificados desde la última copia completa. No es lo más óptimo en cuanto a tiempo y espacio utilizado, pero requiere menos tiempo que la completa y es un proceso más sencillo
incremental: sólo se copian los datos que hayan variado desde la última copia, el espacio y el tiempo utilizados son menores, pero hace la recuperación de datos más compleja.
se utiliza el método 3-2-1 para llegar a la mayor seguridad posible de los datos:
3: mantener 3 copias de cualquier fichero importante,el archivo original y 2 copias de seguridad
2: almacenar las copias en DOS soportes distintos de almacenamiento para protegerlas ante distintos riesgos
1: almacenar UNA copia de seguridad fuera de nuestra empresa, lo que también se conoce como backup offsite. Como la copia en la nube

Borrado seguro de la información

Además se debe conseguir un borrado seguro de la información, es decir, destruirla de forma segura para que no vuelva a ser accesible, el primer paso es realizar un inventario de activos para que ninguno se pierda, después para eliminar la información, deberán triturarse todos los medios de almacenamiento no electrónicos, los dispositivos que permitan su reutilización, deberán ser

sobreescritos múltiples veces, los teléfonos móviles, se cifran antes de ser borrados y se restaurarán a formato de fábrica, los soportes que no funcionen, deberán ser destruidos o desmagnetizados.

Correos fraudulentos

Para defendernos de los ataques por correos fraudulentos deberemos conocer los tipos que existen:

el phishing: suplantación de una entidad fiable para hacerse con claves de acceso o información sensible.

Scam: se basa en perpetrar engaños y estafas

sextorsión: extorsionar al receptor con un supuesto video de contenido privado o comprometedor, que probablemente no exista, y amenazar con difundirlo

malware: se trata de código malicioso oculto, que podría infectar dispositivos

A menudo este tipo de correos muestran un patrón que les relaciona entre sí, suelen ser de remitente desconocido, que a pesar de que no lo sean, existen herramientas que pueden detectar el email spoofing (remitente y firma falsos) o la ausencia o cambio de firma. El objetivo de estos correos es instar al usuario a que realice una determinada acción mediante el uso de ingeniería social en el cuerpo y asunto del mensaje.Las comunicaciones impersonales, documentos adjuntos, faltas de ortografía y mala redacción deben ser signos de alerta, así como el uso de enlaces, cuyo destino debe ser comprobado antes de abrir, para mayor facilidad la mayoría de clientes de correo cuentan con herramientas para ese fin.

Aun así, los ciberdelincuentes pueden no ser siempre el problema, los errores de los empleados como el uso de la función de autocompletado, que podría resultar en el envío de un correo a un destinatario erróneo o la descarga automática de archivos pueden suponer un problema.

CONTRASEÑAS

Algo que sabes: contraseñas, preguntas personales, etc.

Algo que eres: huellas digitales, iris o retina, voz, etc.

Algo que tienes: tokens criptográficos, tarjeta de coordenadas, etc.

Longitud mínima de 8 caracteres, ya que cuanto más larga sea esta, más tiempo se tardará en descubrir la;

Utilizar combinaciones de letras mayúsculas, minúsculas, números y símbolos.

Una forma de conseguir contraseñas robustas es utilizar reglas mnemotécnicas aplicadas a una frase:

Seleccionamos una frase: «en un lugar de la mancha»;

Hacemos uso de mayúsculas: «En un lugar de la Mancha»;

Incluimos el servicio: «En un lugar de la Mancha Correo»;
Añadimos números: «En un lugar de la Mancha Correo de 2019»;
Añadimos caracteres especiales: «En un lugar de la Mancha Correo de 2019!»;
Podemos comprimirla para hacerla más fácil de recordar, utilizando, por ejemplo, la primera letra de cada palabra, de tal forma que quedara: «EuldlM d2019!».

PUESTO DE TRABAJO

Riesgos a los que se expone el puesto de trabajo:
Información en papel al alcance de cualquiera.
La falta de confidencialidad de los medios de comunicación tradicionales como el teléfono.
Accesos no autorizados a los dispositivos.
Infecciones por malware.
Robo de información, etc...

Mesas limpias

Al acabar la jornada se debe guardar la documentación que se encuentre a la vista.
Se debe prestar especial atención a que:
El puesto de trabajo está limpio y ordenado.
La documentación que no se utilice en un momento determinado debe estar guardada correctamente, especialmente cuando se abandona el puesto de trabajo o se finaliza la jornada.
No hay usuarios ni contraseñas apuntadas en post-it o similares.
Bloqueo de sesión:
Windows= Win + L
MacOS= control + opción + q
Linux= Ctrl + alt + L
Hace falta tener el software actualizado y el antivirus y Firewall son las herramientas de Seguridad que protegen al equipo del software malicioso.

PUESTO DE TRABAJO

Contrato de confidencialidad:
Indicar qué información se considera confidencial y por lo tanto está protegida por el acuerdo.
Fijar la duración de la relación de confidencialidad, que generalmente será superior al tiempo de prestación del Servicio.
En caso de ser necesario, se indicará la jurisdicción legal a la que se acoge cada una de las partes.
Acceder a sitios de dudosa legitimidad como webs de descargas, juego, adultos, etc., no es un uso lícito de los recursos empresariales.
Software legítimo
Programas pirata o adquiridos de forma fraudulenta podrían conllevar sanciones económicas y penales.

Software ilegal puede terminar en una infección por malware del equipo.
Cómo y cuándo reportar un incidente de Seguridad
Acceso no autorizado a sistemas o información, como en el caso de robo de un dispositivo o de las credenciales de acceso.
Denegaciones de servicio, en las cuales el incidente impide el correcto funcionamiento de un recurso, como por ejemplo la página web de la empresa.
Infección por malware.
Robo de información de la empresa.
Uso seguro de dispositivos de almacenamiento extraíbles
Tenemos que minimizar las situaciones de riesgo si su uso está permitido en la empresa y saber en qué situaciones se pueden utilizar y qué información se puede llevar en estos dispositivos, para ello se utilizarán métodos seguros de borrado y destrucción de soportes.

BYOD TELETRABAJO

El robo o pérdida de los móviles, tabletas, portátiles y dispositivos de almacenamiento como discos duros externos y pendrives. Este puede ser el riesgo más importante al que se exponen estos dispositivos debido a su tamaño y en muchos casos, a su elevado coste.
La infección por malware siempre es un riesgo a tener en cuenta, pues el software malicioso puede robar información confidencial de la empresa y credenciales de acceso a diferentes recursos. A menudo descuidamos la protección antimalware en equipos pequeños.
Los sitios web fraudulentos, la publicidad agresiva o las páginas web de tipo phishing son las principales amenazas a las que se exponen. Navegar en dispositivos pequeños, particularmente en móviles, entraña riesgos al ser más difícil «librarse» de esta publicidad.
Utilizar redes wifi inseguras puede poner en riesgo la privacidad de las comunicaciones, ya que los ciberdelincuentes pueden estar «escuchando» todo lo que se envía y recibe. También podemos conectarnos a redes wifi que suplantan a redes wifi lícitas.
Instalar aplicaciones que necesitan acceder a determinados permisos del dispositivo, en ocasiones excesivos o innecesarios (como acceso a la cámara, los contactos o los archivos), para poder funcionar con normalidad, pudiendo así verse la información empresarial comprometida.
Dispositivos que no cuentan con controles de acceso robustos que los protejan de un descuido, robo o pérdida. La ausencia de los mismos o el uso de algunos considerados débiles, como el patrón de bloqueo, son un riesgo para su seguridad.
Tanto el sistema operativo, como las aplicaciones desactualizadas suponen un riesgo para la seguridad de toda la información que gestionan.
La modificación de los controles de seguridad impuestos por los fabricantes. Algunos usuarios deciden rootear o hacer jailbreak a sus dispositivos lo que puede

suponer un grave riesgo, ya que los controles de seguridad impuestos por el desarrollador son eliminados.
Establecer que el dispositivo o la aplicación recuerde la contraseña. Si un tercero accede al dispositivo tendría acceso a todos los servicios en los que estuviera guardada la contraseña.
Utilización de servicios en la nube. La utilización de servicios en la nube o cloud puede suponer un riesgo, ya que la información de la empresa será almacenada en un tercero al que hemos de trasladar nuestros requisitos de confidencialidad, integridad y privacidad. Además, existe el riesgo de que si no fuera posible conectarse a Internet (problemas en la red como congestión o caída de la misma) la información almacenada en la nube no será accesible.
Contraseña de firmware, si el dispositivo lo permite, sobre todo en ordenadores portátiles. De esta forma, se evita que otros usuarios arranquen el equipo desde otro disco distinto del especificado.
Creación de cuentas de usuario y permisos.
En los sistemas operativos como Windows, MacOS o los basados en Linux, se permite la creación de distintos usuarios, otorgándoles una sèrie de privilegios acordes con su perfil. Es recomendable que cada usuario cuente con los privilegios mínimos y necesarios que le permitan desempeñar su trabajo. Además, deberán contar con una contraseña de acceso robusta.
Bloqueo de dispositivos. En los dispositivos basados en Android o iOS hay que establecer el bloqueo de pantalla en el menor tiempo posible y una contraseña de desbloqueo robusta. También pueden utilizarse métodos biométricos como la huella dactilar.
Activar el cifrado de la información en el dispositivo. Todos los sistemas operativos deberán contar con herramientas de cifrado que protegen la información en ellos alojada. Los actuales sistemas operativos móviles como Android e iOS cuentan con cifrado de la información por defecto, pero los sistemas operativos para ordenador no, por lo que se debe activar.
Establecer cuál será el tratamiento aceptable de la información confidencial. Preferiblemente, se accederá a la misma por medio de Internet y se evitará siempre descargar en el dispositivo.
No se permitirán usos domésticos (juegos, descargas, etc.) por otros usuarios en el dispositivo utilizado como puesto de teletrabajo;
Se realizarán copias de seguridad de forma periódica; en caso de utilizar una conexión wifi doméstica que podamos configurar de forma segura [Ref. - 9] Tendremos en cuenta: utilizar cifrado WPA2 o WPA 3 en caso de estar disponible y que los dispositivos sean compatibles; utilizar una clave robusta; desactivar la función WPS en caso de estar activa.
Distracciones de los empleados. Al utilizar un mismo dispositivo para tareas personales y laborales, la productividad puede disminuir al acceder a páginas web no relacionadas con su actividad profesional, redes sociales o la cuenta privada de correo electrónico.

Aumento de las posibilidades de accesos no autorizados a información empresarial, ya que el dispositivo se usa para trabajar y para uso personal. Por lo tanto, las posibilidades de pérdida o robo aumentan y por consiguiente, también aumentan los accesos no autorizados.
El dispositivo puede ser prestado a un amigo o familiar para realizar cualquier tarea, lo que puede poner en riesgo la seguridad de la información de la empresa.
La relación contractual entre empleado y empleador puede llegar a su fin pudiendo ser un riesgo para ambas partes conservar información empresarial una vez ha terminado el contrato.
Ponerlo en conocimiento de la empresa para que se tomen todas las medidas necesarias que eviten el uso indebido del dispositivo y de la información que contiene o a la que tiene acceso.
Si el dispositivo ha sido robado, se deberá interponer una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado [Ref. - 7], aportando toda la información posible.
Bloquear el dispositivo de manera remota. La mayoría de sistemas operativos tanto para ordenador, como para móvil cuentan con herramientas que lo permiten, generalmente a través de un panel de administración web.
Geolocalizar el dispositivo. Actualmente, los dispositivos con sistema operativo Windows, MacOS, Android e iOS cuentan con herramientas que permiten conocer su posicionamiento aproximado.
Siempre que sea necesario se debe tener habilitado en dispositivos empresariales que use el trabajador.
El empresario tiene que avisar a los empleados de forma clara, expresa e inequívoca, tal y como indica la
LOPD GDD 3/2018.
En caso de no ser posible, recuperar el dispositivo se debe optar por realizar un borrado remoto del mismo, de tal manera que toda la información que contenga no pueda estar accesible. Para ello, tendremos habilitada esta opción.

EL VALOR DE LAS REDES SOCIALES:

Mediante la analítica del uso de las redes sociales se pueden obtener datos sobre las características de los seguidores como género, edad o ubicación y sus preferencias de uso, que pueden ser útiles a la hora de lanzar una determinada campaña comercial, maximizando los beneficios de esta.
También son una buena herramienta para captar nuevos clientes y conocer lo que piensan sobre tus servicios o productos.
Permiten aumentar el tráfico web haciendo que la web de la empresa se posicione mejor en los buscadores y aumentando así su visibilidad.

Sirven para potenciar la marca con la colaboración de los propios usuarios de la red social.

Fraude por suplantación de clientes o proveedores. Los ciberdelincuentes pueden crear perfiles falsos suplantando a un cliente o proveedor para modificar datos en su beneficio. Podría modificar, por ejemplo, la cuenta de facturación, direcciones de envío, etc.
Campañas de malware. El envío de software malicioso por medio de los perfiles en redes sociales también es utilizado por los ciberdelincuentes para infectar los equipos de las víctimas. Para engañar a las víctimas utilizan diferentes técnicas como hacerse pasar por un cliente, un proveedor o incluso por alguien de la empresa. Terminan dirigiendo a la víctima a sitios web maliciosos donde descargaron el malware al hacer clic en un anuncio o simplemente para visitarla. En otros casos, lo envían adjunto en mensajes privados dando como resultado, en ambos casos, la infección del equipo.
Campañas de phishing. Los ciberdelincuentes pueden hacerse pasar por una marca conocida y redirigir a la víctima a una página web fraudulenta donde robar información personal, bancaria y datos de la empresa.
lanzar comentarios inoportunos, negativos o inapropiados, como
quejas laborales; emitir juicios de valor; enfrascarse en discusiones sin sentido, insultar, amenazar o acosar; propagar noticias falsas; dar información confidencial o sujeta a propiedad intelectual, etc.

Políticas de empresario

Gestión de recursos humanos

Debemos ser conscientes de que el error humano es la causa más frecuente de fallos de seguridad en una empresa, para solucionar esto se deben tomar medidas de seguridad en la gestión de contratos, firmas, realizar filtros y controles de ciberseguridad, concienciar a los trabajadores y formarlos en seguridad.
Los objetivos de este proceso es asegurarnos de que los trabajadores tienen sus derechos, deberes y responsabilidades así como tienen sus correspondientes sanciones si cometen cualquier infracción.
La gestión de recursos humanos tiene una serie de controles para seguir la medida de seguridad:

Cláusulas contractuales: El empresario junto al departamento de recursos humanos deben establecer ciertos aspectos que serán relevantes en la seguridad de la empresa y serán reflejados en el contrato del trabajador, estos aspectos considerarán también la propiedad intelectual y los datos personales.

Acuerdos de confidencialidad: Tanto los trabajadores como los colaboradores deberán firmar un acuerdo conforme a la información de la empresa, este deberá constar de las partes que intervienen, de la información confidencial, los compromisos de todas las partes y las sanciones y legislaciones.

Revisar las referencias de los candidatos: En puestos con acceso a información muy confidencial, se detallaran las comprobaciones a realizar en el candidato, se determinarán las referencias revisadas y que datos deben verificarse, también indicaremos los puestos concretos libres de antecedentes penales.

Plan de formación y concienciación en ciberseguridad: Estipular actividades para mantener informada a la plantilla sobre la seguridad.

Política de sanciones y expedientes: Elaborar un procedimiento que establezca las sanciones en caso de negligencia en seguridad de la información, ha de ser accesible para los empleados en todo momento.

Finalización del contrato: Comunicar a los empleados las obligaciones de confidencialidad una vez finalice su contrato.

Concesión autorizada de los permisos de acceso: Dar de alta a cada empleado en su control de acceso correspondiente, para ello haremos lo siguiente: entregar las tarjetas de acceso físico, asignar cuentas de correo electrónico, conceder permisos de acceso a servicios, aplicativos y recursos compartidos y asignar el puesto de trabajo, los dispositivos y los equipos.
Revocación de permisos de acceso: Al terminar un contrato se deberá recoger la tarjeta de acceso y los dispositivos, eliminar las cuentas de correo y eliminar los permisos de acceso al sistema.

Aceptación de cláusulas y políticas de seguridad de la información: Cada empleado debe leer y firmar cada documento relacionado con la política de seguridad de la información.

Aprovechamiento de las sesiones formativas de concienciación: Aprovechar las sesiones de formación a disposición de los empleados para comprender riesgos de ciberseguridad.

Almacenamiento en la red corporativa

La empresa dispone de servidores de almacenamiento en red donde almacenar el resultado de los trabajos, los controles de acceso a esta información son definidos por la dirección y el responsable de sistemas.

La información almacenada se determina a través de la política de clasificación de la información y se presta especial atención a información catalogada como crítica o si está sujeta a requisitos legales.

El objetivo es conseguir un buen uso de los servidores y concienciar a los empleados sobre la relevancia de la información y cómo almacenarla.

Controles a revisar de la política de seguridad:

Inventario de los servidores de almacenamiento: Informar a los empleados sobre qué servidores hay y que se almacenan en ellos.

Criterios de almacenamiento:Informar sobre el almacenamiento corporativo, quien puede acceder y cuando se elimina la información.

Clasificación de la información: Informar sobre cumplir la política de clasificación de la información.

Control de acceso: Establecer quién puede acceder a los discos y llevar un control de ello

Copias de seguridad: Hacer un plan de copias de seguridad donde detallar la información que se guarda, donde se guarda, cada cuando se guarda y cuanto tiempo se conserva.

Acceso limitado: Permitir el acceso solo a las zonas necesarias para el trabajador.

Almacenamiento clasificado: Crear las carpetas organizadamente según la política de la empresa y asignar los permisos imprescindibles a los empleados.

Auditoría de servidores: Revisar el estado de los servidores.

Cifrado de la información: Cifrar la información crítica.

Almacenamiento en los equipo de trabajo

Los trabajos guardados de manera local en los dispositivos de la empresa deben disponer de una política de regulación que determine el tratamiento de la información, que se ha de cifrar y cuando y quien controla esa información.

El objetivo es mantener la información local de forma segura y especificar los procedimientos a seguir a los empleados.

Los controles relativos en el almacenamiento en los equipos de trabajo son:

Que se puede almacenar en los equipos corporativos:Crear una normativa que regule el almacenamiento personal.

Donde se guarda la información: Informar de donde se debe guardar la información dentro de los directorios del equipo.

Conservación de la información en discos locales: Determinar el tiempo que se conserva la información local antes de eliminarla o transferirla.

Permanencia de la información en discos locales una vez transferida a los servidores: Determinar el tiempo de la información local en los servidores antes de ser eliminada.

Cifrado de información: Cifrar información crítica antes de guardarla.

Conocimiento y aplicación de la normativa: Conocer y aplicar la normativa.

Almacenamiento en la nube

La empresa ha de dispone de una política de clasificación de la información que indique que puede subirse a la nube y a de transmitirla en todo momento a los trabajadores para que estos hagan un buen uso de los recursos de almacenamiento disponibles

El objetivo de esto es utilizar eficazmente el espacio en la nube y maximizar la seguridad de la información

Los controles relativos en el almacenamiento en la nube son:

Uso de servicios de almacenamiento en cloud públicas: Informar sobre las restricciones en clouds públicas a los trabajadores.

Lista de servicios cloud permitidos: Elaborar una lista con los clouds permitidos para los trabajadores.

Proceso de borrado de la información en la nube: Informar sobre los procesos de borrado adecuados para la información en la nube.

Tipo de información almacenada y tratamiento: Informar de qué información puede ser almacenada en la nube y si ha de estar cifrada.

Copias de seguridad en la nube: Valoración de ventajas o desventajas al almacenar las copias de seguridad en la nube.

Contratación de servicios de almacenamiento en la nube: Contratar un servicio cloud que se adecue a los criterios de la empresa.

Política de seguridad del proveedor: Conocer las políticas de almacenamiento en la nube del proveedor.

Aplicaciones permitidas

La empresa debe determinar y controlar el software utilizado por sus equipos para evitar riesgos de infecciones, fugas de información y sanciones penales.

El objetivo es controlar que todo el software utilizado sea legal y que sea el autorizado por la empresa.

Los controles relativos en las aplicaciones permitidas son:

Registro de licencias: Mantener un registro de licencias de software actualizado.

Competencia para la instalación, actualización y borrado: Nombrar personal técnico que se encargue del software de los equipos de la empresa.

Sanciones por usos no autorizados:Informar al personal sobre las sanciones por usar software no autorizado.

Repositorio de software: Tener un repositorio con todo el software autorizado y sus credenciales.

Auditoría de software instalado: Analizar que el software instalado sea el autorizado y tenga licencia.

Autorización y licencia del software: Utilizar el software autorizado en todos los dispositivos y disponer de sus licencias.

Política de copias de software: No realizar copias de software sin consentimiento.

Clasificación de la información

La empresa debe realizar un inventario y clasificar cada activo de información dependiendo de su impacto respecto a la empresa aplicando para ello criterios de confidencialidad, integridad y disponibilidad, también deberá establecer un tiempo un ciclo de vida dependiendo de la vigencia y de la vida útil del soporte.

El objetivo es garantizar una gestión eficaz de la seguridad de la información.

Los controles relativos en la clasificación de la información son:

Inventario de la información: Elaborar un inventario detallado de la información de la empresa.

Criterios de clasificación de la información: Determinar los criterios de seguridad para clasificar la información.

Clasificación de la información: Etiquetar la información según los criterios de seguridad.

Tratamientos de seguridad disponibles: Establecer una lista con los tratamientos de seguridad disponibles para la empresa.

Establecer y aplicar los tratamientos que corresponden a cada tipo de información: Aplicar los tratamientos de seguridad correspondientes a cada información.

Auditorías: Realizar auditorías de comprobación cada cierto tiempo.

Concienciación y formación

La dirección de la empresa debe poner total compromiso con la formación de los empleados, siendo consciente de la formación proporcionada y revisar periódicamente para prevenir incidentes y adaptarse a las nuevas tecnologías.

El objetivo es asegurarse de que los trabajadores conozcan, entiendan y cumplan las normas y las medidas de protección en ciberseguridad.

Los controles relativos en la concienciación y formación son:

Difusión de la política de seguridad: Documentar y difundir las normas de ciberseguridad.

Concretar el plan de formación: Elaborar y revisar los planes de formación en ciberseguridad de los trabajadores.

Programas de formación específicos: Desarrollar programas de formación en ciberseguridad dependiendo de cada puesto de trabajo.

Periodicidad de la formación: Cada cierto tiempo deben realizarse cursos o charlas para los empleados.

Evaluar el aprendizaje obtenido: Comprobar el conocimiento asimilado por los empleados.

Promover una cultura de seguridad de la información: Promover la seguridad de información en la cadena de suministros de la empresa y los clientes.

Continuidad de negocio

La empresa debe tener un plan de continuidad de negocio que debe tener en cuenta a las personas responsables de aplicarlo, a las operativas a seguir, a los activos implicados y las indicaciones.

Debe comprobarse que los servicios tecnológicos que se contraten tengan planes de contingencia que se adecuen a nuestra empresa.

El objetivo es diseñar y probar un plan que nos permita recuperar la operatividad habitual de la empresa en un tiempo razonable.

Los controles relativos en la continuidad del negocio son:

Determinar el alcance del PNC: Analizar la continuidad de los activos y los procesos.

Concretar el flujo de responsabilidades: Determinar las responsabilidades de las personas responsables del PCN en caso de desastres.

Realización del BIA(Análisis del impacto en el negocio): Elaborar detalladamente el BIA

Definir la política de comunicación y aviso a entidades externas: Definir el tipo de mensajes que transmite la empresa si hay un desastre.

Caducidad del PCN: Actualizar el PCN cada cierto tiempo.

Elegir la estrategia de continuidad: Elegir una estrategia óptima de continuidad de la empresa.

Detallar la respuesta a la contingencia: Detallar los controles y procedimientos a ejecutar en un desastre.

Desarrollar actividades para verificar, revisar y evaluar el plan de continuidad del negocio: Probar y evaluar el PCN cada cierto tiempo.

Cumplimiento legal

La empresa debe conocer las responsabilidades del complimiento legal y que consecuencias puede tener su incumplimiento.

El objetivo es asegurar el conocimiento y cumplimiento de las obligaciones legales sobre seguridad de la información.

Los controles relativos en el cumplimiento legal son:

Definir y documentar la manera de cumplir con todos los requisitos legales: Detallar los procedimientos a seguir para cumplir la legislación sobre ciberseguridad

Garantizar el cumplimiento de los derechos de propiedad intelectual de terceros: Controlar la compra y el uso de software de tu empresa para que este cumpla la ley de propiedad intelectual.

Garantizar el cumplimiento de los derechos de propiedad intelectual propios: Revisar que se respeten los derechos sobre las obras de la empresa.

Comprobar si tu empresa realiza una actividad comercial en la UE o trata datos personales en la UE o sobre personas que se encuentren en la UE: Comprobar si alguna actividad necesita una gestión de datos personal.

Determinar las responsabilidades para gestionar la protección de datos personales: Designar un responsable del tratamiento de los datos y revisar los contratos con el.

Revisar el cumplimiento del deber de informar y que los interesados puedan ejercitar sus derechos según el RGPD: El responsable informará sobre el tratamiento, obtener los consentimientos, permitir ejercer los derechos y notificar a las autoridades en caso de brechas.

Realizar una evaluación de impacto si haces tratamientos de alto riesgo para la privacidad: Los tratamientos de alto riesgo tratan datos especiales o a gran escala.

Llevar un registro de actividades de tratamiento: Con más de 250 trabajadores o si tienes tratamientos de alto riesgo, debes realizar el registro de actividades del RGPD.

Establecer un procedimiento para notificar en caso de brecha de seguridad: Actualizar tus procedimientos para avisar de la brecha a las autoridades en un plazo de 72 horas.

Aplicar las medidas organizativas para adecuarse al RGPD: Definir los procedimientos para cumplir el rgpd y ofrecer garantías a los interesados, proporcionar la información a los empleados si van a participar.

Aplicar las medidas técnicas de seguridad adecuadas según el análisis de riesgos para la privacidad: Determinar dónde están los datos y clasificarlos por criticidad, monitorizar el uso, quien accede y cuando se eliminan o se cifran. Garantizar confidencialidad integridad y disponibilidad.

Revisar si tu empresa realiza comunicaciones comerciales que obliguen al cumplimiento de la LSSI: Cumplir con la LSSI garantizando la seguridad en comunicaciones comerciales.

Comprobar los requisitos de la LSSI y el RGPD si tu empresa dispone de comercio electrónico o realiza transacciones online: Mostrar la información de la LSSI en la web. Informar de la política de cookies de la misma.

Garantizar el cumplimiento de los derechos de propiedad industrial y marcas propias y de terceros: Revisar los derechos industriales, marcas y patentes.

Otras regulaciones: Tener en cuenta la existencia de las limitaciones legales que afecten a la seguridad de tu información.

Plan de director de seguridad

La empresa deberá disponer de un PDS, partiendo de un buen análisis y este deberá estar alienado con los intereses de la empresa e incluirá obligaciones y prácticas a cumplir por todos los empleados.

El objetivo es planificar y organizar los proyectos para garantizar la protección de la seguridad de la información.

Los controles relativos en el plan director de seguridad son:

Analizar la situación actual de la empresa: Analizar la situación de la empresa para acometer el PDS.

Alinear el PDS con la estrategia de la empresa: Tener en cuenta la estrategia a la hora de diseñar el PDS.

Definir los proyectos a ejecutar: Establecer acciones concretas para llegar al nivel de seguridad deseado.

Clasificar y priorizar los proyectos: Clasificar las acciones a ejecutar para priorizar las que proporciones mejor beneficio/coste.

Aprobar el PDS: Aprobar y publicar el PDS.

Ejecución del PDS: Poner en marcha los proyectos del PDS.

Certificación en seguridad: Implantar un proceso que acredite el sistema de la gestión de seguridad de la empresa.

Relación con proveedores

La empresa deberá controlar y asegurar la seguridad de los proveedores y exigir la más favorable para la seguridad de ambas partes.

El objetivo es controlar la relación con los proveedores para controlar y proteger nuestra información en base a diversos acuerdos y contratos.

Los controles relativos en la relación con los proveedores son:

Requisitos de seguridad en productos y servicios: Establecer los requisitos mínimos que deben cumplir los servicios que contrates.

Definir cláusulas contractuales en materia de seguridad de la información: Ser riguroso elaborando las cláusulas contractuales.

Definir las responsabilidades concretas por ambas partes: Delimitar las responsabilidades de todas las partes involucradas.

Definir los ANS: Definir los ANS que sometes a los servicios contratados.

Controles de seguridad obligatorios: Determinar que controles serán obligatorios en relación con los servicios de los proveedores.

Formar parte de los foros y organizaciones de usuarios de los productos/servicios software utilizados: Controlar los productos que adquieres y la reputación de los proveedores.

Certificación de los servicios contratados: Exigir a los proveedores los certificados contratados en sus productos.

Auditoría y control de los servicios contratados: Supervisar que los productos correspondan al producto acordado.

Finalización de la relación contractual: Garantizar la seguridad de la información tras finalizar un contrato.

Políticas para el personal técnico

Teletrabajo seguro

La empresa deberá contar con medidas de seguridad adecuadas para no poner en riesgo a la organización ni a los trabajadores teniendo en cuenta las necesidades de la empresa.

El objetivo es garantizar la seguridad de la información y gestionar correctamente los recursos disponibles, a parte de concienciar a los empleados.

Los controles relativos en el teletrabajo seguro son:

Normativa de protección del puesto de trabajo remoto: Informar mediante auditorías, al personal sobre la normativa de protección.

Relación de usuarios que disponen de la opción de trabajar en remoto: Llevar un control de las personas con opción a teletrabajar

Procedimientos para la solicitud y autorización del teletrabajo: Redactar un documento con todas las cuestiones de teletrabajo, ha de ser firmado por los teletrabajadores.

Periodo de implantación y pruebas: Contemplar los riesgos de seguridad antes de habilitar el teletrabajo.

Realizar pruebas de carga en escenarios simulados: Valorar la carga ocasionada en los sistemas internos por los teletrabajadores.

Aplicaciones y recursos a los que tiene acceso cada usuario: Dar y detallar a los teletrabajadores los recursos y condiciones de uso permitidos.

Acceso seguro:Gestionar las credenciales de acceso de los empleados con las normativas de la empresa.

Configuración de los dispositivos de teletrabajo: Configurar los dispositivos utilizados por el teletrabajador.

Cifrado de los soportes de información: Implantar tecnología de cifrado

Definición de la política de almacenamiento en los equipos de trabajo y en la red corporativa: Elaborar políticas sobre el destino de la información.

Planificación de las copias de seguridad de todos los soportes: Comprobar que se realizan y pueden restaurarse.

Uso de conexiones seguras a través de una red privada virtual o VPN: Implementar una VPN extremo a extremo.

Aplicaciones de escritorio remoto siempre a través de una VPN: Permitir el uso de aplicaciones de escritorio remoto solamente con una VPN.

Virtualización de entornos de trabajo: Valorar la virtualización para cada empleado.

Priorizar el uso de dispositivos corporativos: Elegir los dispositivos corporativos para teletrabajar.

Conexión a Internet: Utilizar los datos móviles si no es posible utilizar la red doméstica.

Uso de dispositivos personales bajo una política BYOD: Utilizar las configuraciones y conexiones permitidas para teletrabajar

Concienciar a los empleados antes de empezar a teletrabajar: Formar a los empleados antes de empezar a teletrabajar.

Cumplimiento LOPD GDD: Formar a los empleados para la protección de los datos personales durante el teletrabajo.

Aplicaciones de teleconferencia y colaborativas: Configurar un uso seguro de las aplicaciones para respetar la privacidad y la propiedad intelectual.

Borrado seguro y gestión de soportes

La empresa empresa debe cumplir con la ley de protección de datos destruyendo completamente la información que ya no sea necesaria.

El objetivo es establecer las normas adecuadas para el borrado seguro de la información obsoleta.

Los controles relativos en el borrado seguro y la gestión de soporte son:

Inventario de activos: Realizar un seguimiento de las personas responsables de los dispositivos, de los propios dispositivos y de la información que contienen.

Gestión de soportes: Supervisar los dispositivos que almacenen información corporativa.

Eliminación de la información en soportes no electrónicos: Destruir completamente la información de los soportes no electrónicos.

Eliminación de la información para la reutilización de soportes electrónicos: Reescribir para reutilizar un soporte en buen estado.

Eliminación de la información antes de deshacernos de soportes electrónicos: Desmagnetizar o destruir el soporte de almacenamiento antes de desechar.

Borrado de información en otros dispositivos: Eliminar la información antes de deshacerse de los dispositivos.

Documentación de las operaciones de borrado realizadas: Obtener un documento que verifique el borrado realizado con detalles.

Destrucción certificada: Utilizar un servicio certificado para la destrucción de los datos confidenciales.

Uso de dispositivos móviles corporativos

La empresa debe tomar medidas de seguridad para no ser tan susceptible a los robos de información en caso de una pérdida de dispositivo.

El objetivo es establecer normas de seguridad para un correcto uso de los dispositivos corporativos.

Los controles relativos en el uso de dispositivos móviles corporativos son:

Asignación de dispositivos: Elaborar un procedimiento de solicitud y asignación de los dispositivos.

Registro de equipos: Registrar a quien y cuando se le da un dispositivo, y el software del mismo.

Mantenimiento de dispositivos: Elaborar un formulario de solicitud de cambios en los dispositivos.

Protección de la BIOS: Configurar la BIOS con contraseña.

Software de localización: Comunicar al trabajador si el dispositivo tiene software de localización o si es necesario.

Almacenamiento de la información: No almacenar información corporativa si no es necesaria.

Tratamiento de la información confidencial: Cifrar y eliminar la información confidencial de forma segura.

Conexión a redes: Conectar los dispositivos a redes conocidas o a los datos móviles solamente.

Notificación en caso de infección: Notificar al personal técnico si se sospecha que hay alguna infección en el dispositivo.

Transporte y custodia: Elaborar una serie de requisitos para la seguridad de los dispositivos al ser transportados fuera de un lugar de trabajo seguro.

Uso del puesto de trabajo: Aplicar las políticas del puesto de trabajo relativas a usar un equipo informático.

Responsabilidades: Conocer las responsabilidades y las normas al utilizar un dispositivo corporativo móvil.

Almacenamiento en la nube

La empresa debe establecer una política de control de malware

El objetivo es proteger toda la información contra cualquier infección.

Los controles relativos en antimalware son:

Instalar o contratar una solución antimalware: Analizar qué solución es la más adecuada para la empresa y aplicarla.

Configurar las herramientas de detección de malware: Configurar correctamente las herramientas antimalware.

Actualizar las herramientas de detección de malware: Actualizar cada cierto tiempo las herramientas antimalware instaladas.

Establecer el procedimiento de respuesta ante la infección por ejecución de malware: Elaborar los procedimientos a seguir en caso de infección de malware.

Buenas prácticas para el control de malware: Seguir las directrices de prevención de infecciones.

Auditoria de sistemas

La empresa debe determinar su nivel de seguridad actual y establecer el nivel a conseguir, para ello deberá realizar diferentes auditorias.

El objetivo es obtener las evidencias de que nuestros sistemas cumplen con los niveles de seguridad y avanzan en la mejora de seguridad.

Los controles relativos en la auditoría de sistemas son:

Detallar los elementos clave que queremos que sean auditados: Identificar los activos más relevantes para ser auditados.

Mejora continua y modelos de madurez: Enfocar las auditorías para una mejora continua.

Auditorías legales: Verificar el cumplimiento de los requerimientos del RGPD.

Auditorías forenses: Determinar lo ocurrido tras un incidente.

Procedimientos: Definir procedimientos para auditar la seguridad de los sistemas de información.

Realización de auditorías periódicas: Realizar auditorías de los sistemas de información cada cierto tiempo

Análisis del resultado de la auditoría: Buscar debilidades a corregir

Comercio electrónico

La empresa debe contemplar la seguridad de los clientes y de la propia empresa a la hora de vender productos a través de la web.

El objetivo es verificar que las medidas que se aplican sean las correctas para evitar el fraude y garantizar la seguridad de los clientes.

Los controles relativos en el comercio electrónico son:

Cumplimiento de políticas relacionadas: Cumplir la política de seguridad web y la política de relación con los proveedores.

Certificado web con validación extendida: Adquirir un certificado con validación externa para la tienda online.

Sellos de confianza para el comercio electrónico: Obtener sellos de confianza para garantizar la seguridad de la web.

Medidas de carácter legal: Asegurarse de que la web cumple con las medidas legales.

Prevención de compras fraudulentas: Elaborar listas blancas y negras de los clientes.

Pago virtual con tarjetas de crédito: Cumplir con el estándar de seguridad de datos para la industria de tarjeta de pago.

Control de acceso: Aplicar la política de control de acceso y de contraseñas para acceder al gestor de la web.

Detección de compra fraudulenta: Comprobar los intentos de compra.

Prevención del fraude: comprobaciones a realizar para aceptar nuevos clientes: Comprobar si los datos están en la lista negra o si tiene registros de fraude anteriores.

Prevención de fraude: comprobaciones a realizar para clientes registrados: comprobar si los datos están en la lista blanca, si hay algún problema de pago y si los datos coinciden con pedidos anteriores.

Actuación ante la detección de compra fraudulenta: No enviar el producto, contactar y comprobar la transacción y acudir a las FCSE para interponer una denuncia.

Control de acceso

La empresa debe controlar quien accede a la información de la misma y tener un registro de quien accede para analizar los posibles incidentes de seguridad.

El objetivo es establecer qué personal puede acceder a qué tipo de información y cuándo accede.

Los controles relativos en el control de acceso son:

Política de usuarios y grupos: Definir a los trabajadores en función de la información a la que acceden.

Asignación de permisos: Asignar los permisos necesarios a cada trabajador.

Creación/modificación/borrado de cuentas de usuario con permisos: Definir un procedimiento para modificar las cuentas de usuario.

Cuentas de administración: Gestionar las cuentas de administración teniendo en cuenta su criticidad.

Mecanismos de autentificación: Implantar las técnicas de autenticación más adecuadas para el criterio de la empresa.

Registro de eventos: Registrar todos los eventos relevantes en el manejo de la información de la empresa.

Revisión de permisos: Revisar cada cierto tiempo que los permisos sean los correspondientes.

Revocación de permisos y eliminación de cuentas: Desactivar los permisos y eliminar las cuentas una vez finalizada la relación contractual.

Copias de seguridad

La empresa debe realizar un inventario de activos de información y clasificarlos en base a su criticidad, la empresa ha de identificar a los responsables de los backups y ha de definir los procedimientos para las copias y restauraciones.

La empresa ha de llevar un control de los soportes utilizados y quién puede acceder a ellos.

El objetivo es verificar y garantizar la continuidad del negocio.

Los controles relativos en las copias de seguridad son:

Inventario de activos de información: Mantener un inventario de los activos y clasificarlos según la criticidad.

Control de acceso: Controlar el acceso a las copias de seguridad.

Copias de seguridad de la información crítica: Hacer copias de la información crítica y la exigida por la ley.

Periodicidad de las copias de seguridad: Realizar copias de seguridad cada cierto tiempo.

Tipo de copia apropiada: Hacer copias de seguridad dependiendo de lo que sea necesario para la empresa.

Caducidad de las copias de seguridad: Conservar las copias de seguridad durante un tiempo estipulado.

Ubicación de las copias de seguridad: Guardar una copia completa fuera de la organización y guardar copias en una caja ignífuga y bajo llave.

Copias en la nube: Tomar las medidas de seguridad necesarias con el proveedor.

Procedimientos de copia y restauración: Aplicar los procedimientos elaborados y revisarlos anualmente y con cada cambio en los activos.

Comprobar que las copias están bien realizadas y que pueden restaurarse: comprobar cada cierto tiempo la fiabilidad de las copias.

Soporte de las copias de seguridad: Revisar que el soporte para hacer la copia es adecuado y esta en buen estado.

Control de los soportes de la copia: etiquetar y llevar un registro sobre los soportes en los que se haya realizado alguna copia.

Destrucción de soportes de copia: Destruir de forma segura los soportes desechados.

Cifrado de las copias de seguridad: Cifrar las copias de seguridad con información confidencial y las subidas a la nube.

Gestión de logs

La empresa necesita un sistema que registre la actividad de los usuarios y los procesos internos constantemente.

El objetivo es determinar eventos dentro del sistema y detectar intrusiones o errores.

Los controles relativos en los logs son:

Que actividad debe ser registrada: Analizar qué eventos quieres registrar.

Información relevante incluida en el registro: Determinar la información más significativa a almacenar.

Formato de la información registrada: Detallar el formato de los logs.

Elección del mecanismo de registro: Seleccionar el sistema más apropiado para la empresa.

Protección y almacenamiento: Proteger la información registrada en los logs.

Sincronización del reloj: Revisar la sincronización temporal de todos los dispositivos.

Sistemas de monitorización y alerta: Configurar los sistemas para generar en tiempo real alertas.

Protección de la página web

La empresa ha de tener en cuenta las medidas de seguridad apropiadas de su empresa para contratar a los proveedores que diseñen la página web.

El objetivo es proteger la página web de posibles ataques y cumplir con la legislación garantizando la seguridad de nuestros clientes.

Los controles relativos en la protección de la página web son:

Certificado web: Proteger mediante cifrado los canales por los que se transmite la información.

Información del usuario: Aplicar las normas del RGPD.

Desarrollo de terceros: Tener los criterios de seguridad en el desarrollo de terceros.

Cumplimiento legal: Cumples los aspectos legales de LSSI y LPI.

Alojamiento en servidor propio: Disponer de medidas de seguridad.

Alojamiento en servidor externo: Asegurar que se sigan las medidas pactadas con el proveedor.

Administración por terceros: Mantener un registro de la actividad.

Configuración del CMS: Aplicar medidas de seguridad.

Acceso al panel de control: Asegurar que las claves de acceso cumplan los criterios de seguridad.

Limitación de accesos: Configurar los servidores con un máximo de accesos a la vez.

Usuarios por defecto: Eliminar los usuarios por defecto

Guardado de registros: Guardar cualquier interacción durante un cierto tiempo.

Comercio electrónico: Elaborar una normativa siguiendo la política de comercio electrónico.

Sellos de confianza: Disponer del sello de confianza que acredite la seguridad de la web.

Copias de seguridad: Realizar copias de seguridad periódicas.

Auditorías: Realizar auditorías externas.

Software actualizado: Actualizar cada cierto tiempo el CMS, sus complementos y el software del servidor.

Protección frente al malware: Instalar antivirus en los equipos.

Respuesta a incidentes

La empresa deberá preparar un plan de acción para los incidentes de ciberseguridad.

El objetivo es asegurarnos de que todos los trabajadores actúen correctamente ante cualquier incidente.

Los controles relativos en la respuesta a incidentes son:

Equipo responsable: Seleccionar el equipo encargado de gestionar los incidentes.

Mejora continua: Adoptar mejoras gracias a la información recogida.

Caducidad del plan de gestión: Revisar cada cierto tiempo el plan de gestión y la respuesta del mismo.

Detección del incidente: Concretar las situaciones catalogadas como incidentes.

Evaluación del incidente: Categorizar los incidentes por criticidad.

Notificación del incidente: Establecer una buena manera de notificar el incidente.

Resolución del incidente: Desarrollar procedimientos de actuación detallados.

Tratamiento del registro del incidente: Registrar toda la información relativa del incidente.

Cumplimiento del RGPD: Tener prevista una notificación del incidente si éste afecta a datos personales.

Uso de técnicas criptográficas

La empresa debe proteger la información sensible y confidencial cuando está en tránsito o almacenada, deberá garantizar la confidencialidad e integridad de la información y deberá utilizar protocolos seguros en las comunicaciones.

El objetivo es garantizar el uso adecuado de estas técnicas para asegurar la confidencialidad, integridad y autenticidad de la información de la empresa.

Los controles relativos en el uso de técnicas criptográficas son:

Información susceptible de ser cifrada: Identificar la información a cifrar.

Uso de firma electrónica: Implantar su uso en acuerdos comerciales.

Certificados web: Adquirir un certificado web.

Cifrado de datos sensibles cuando se contratan servicios externos: Comprobar que se utilizan los canales y las herramientas dadas para cifrar la información.

Cifrado de datos sensibles cuando se solicitan desarrollos de aplicaciones: Comprueba que se cifren las credenciales acordadas.

Acceso desde el exterior con VPN: Autorizar el acceso mediante canales de VPN cifrados.

Algoritmos de cifrado autorizado: Aplicar los algoritmos más adecuados para tus sistemas.

Aplicaciones autorizadas para usos criptográficos: Disponer de una lista de aplicaciones para el cifrado.

Uso de protocolos seguros de comunicación: Implementar protocolos para acceder a los servidores.

Cifrado de la wifi de la empresa: Configurar la wifi con el cifrado más seguro, WPA2.

Actualización de software

La empresa deberá mantener actualizados los equipos y las aplicaciones teniendo en cuenta la vida útil de los dispositivos.

El objetivo es elaborar procedimientos que permitan instalar las actualizaciones de forma segura y controlada.

Los controles relativos en la actualización de software son:

Determinar el software que debe ser actualizado: Realizar un listado del software de la empresa.

Determinar cuándo y qué actualizaciones instalar: Revisar las actualizaciones antes de instalarlas.

Probar las actualizaciones: Contrastar las actualizaciones en un entorno de pruebas.

Deshacer los cambios: Contar con procedimientos para deshacer los cambios después de una actualización.

Herramientas de diagnostico y actualizacion: Utilizar herramientas de autodiagnóstico en los equipos.

Configuración de un sistema de alertas: Configurar un sistema de alertas para recibir avisos de vulnerabilidades.

Registro de actualizaciones: Registrar cada actualización instalada.

Almacenamiento en los dispositivos extraíbles

La empresa deberá aplicar medidas de seguridad para los dispositivos de almacenamiento extraíble, deberá decidir si permite su uso y deberá disponer de su correspondiente normativa.

El objetivo es establecer ciertas normas con respecto a los dispositivos extraíbles para mejorar la seguridad.

Los controles relativos en el almacenamiento en los dispositivos extraíbles son:

Normativa de almacenamiento en dispositivos extraíbles: Elaborar una normativa para el uso de estos dispositivos.

Concienciación de los empleados: Involucrar a los empleados en la protección de los dispositivos.

Alternativas a los medios de almacenamiento extraíble: Implementar alternativas para no utilizar los dispositivos extraíbles.

Registro de usuarios y dispositivos: Mantener un registro actualizado.

Aplicar medidas técnicas para garantizar un almacenamiento seguro de la información en el dispositivo extraíble: Aplicar medidas para el almacenamiento seguro.

Aplicar medidas técnicas para garantizar un almacenamiento seguro de la información en los dispositivos a los que se conecta: Aplicar medidas seguras en los dispositivos a los que se conecta.

Aplicar medidas técnicas para garantizar un almacenamiento seguro de la información sobre los documentos: Aplicar medidas seguras en los documentos que se transfieren.

Cumplimiento de la normativa: Conocer y aceptar la normativa corporativa del uso de dispositivos extraíbles.

Políticas para el empleado

Contraseñas

La empresa debe garantizar que las credenciales de autenticación se generen, actualicen y se revoquen de forma óptima y segura estableciendo un procedimiento claro para llevarlo a cabo.

El objetivo es establecer y difundir las buenas prácticas en las contraseñas.

Los controles relativos en las contraseñas son:

No utilizar las contraseñas por defecto: Ir cambiando las contraseñas de la empresa.

Contraseñas robustas: Generar contraseñas teniendo en cuenta su fortaleza.

No hacer uso del recordatorio de contraseñas: No usar nunca el apartado de recordatorio .

Doble factor para servicios críticos: Incorporar sistemas de autenticación multiplataforma.

No utilizar la misma contraseña para diferentes servicios: Variar las contraseñas por cada servicio utilizado.

Utilizar gestores de contraseñas: Usar gestores de contraseña seguros para poder recordarlas.

No compartir las contraseñas con nadie: Mantener en secreto las claves y no decirlas a nadie.

Cambiar las contraseñas periódicamente: Hacer que las contraseñas se cambien cada cierto tiempo.

Gestión de contraseñas: Definir un sistema de gestión de contraseñas avanzado

Técnicas de autenticación externas: Consideración de la utilización de autenticadores externos.

Herramientas para garantizar la seguridad de las contraseñas: Ayudarse de técnicas y herramientas informáticas.

Uso de dispositivos móviles no corporativos

La empresa debe garantizar que los dispositivos móviles se utilizan de forma segura y cautelosa en las instalaciones de la empresa y fuera de ella.

El objetivo es establecer y difundir las buenas prácticas de los dispositivos móviles.

Los controles relativos de los dispositivos móviles son:

Normas y procedimientos BYOD: Elaborar normas y procedimientos si permitimos el BYOD en la empresa.

Prohibición de uso de dispositivos manipulados: Prohibir el uso de dispositivos rooteados o a los que se le ha aplicado el jailbreak.

Concienciación de los empleados: Involucrar a los empleados a su propia protección de sus dispositivos.

Formación de los empleados: Proporcionar charlas y cursillos para los empleados

Limitar el acceso a redes externas: Prohibición del uso de redes externas e inalámbricas.

Listado de aplicaciones no permitidas: Mantener un listado de aplicaciones no permitidas en la empresa

Controlar el almacenamiento en la nube de datos corporativos: Supervisar el almacenamiento en la nube

Proceso de borrado de la información: Aplicación de una normativa de eliminación de datos.

Control de usuario y dispositivos: Mantener un riesgo actualizado con usuarios, dispositivos y privilegios de acceso.

Aplicar medidas técnicas para garantizar un almacenamiento seguro de la información: Instalación de medidas de seguridad para mantener seguro el almacenamiento de datos.

Bloqueo programado: Tras un periodo de inactividad programar un bloqueo del dispositivo.

Desconexión wifi y Bluetooth: Desactivación de la búsqueda de señal wifi y bluetooth en tu dispositivo .

Cumplimiento de la normativa: Conoces y sigues la normativa para una buena ejecución.

Control de acceso a la red: Implantación de un control de red para mayor seguridad.

Extravío de dispositivos: Configuración de medidas de seguridad para la protección de información corporativa.

Uso del correo electrónico

La empresa debe garantizar que el correo electrónico se utiliza de forma segura y cautelosa en las instalaciones de la empresa y fuera de ella.

El objetivo es establecer y difundir las buenas prácticas del correo electrónico.

Los controles relativos del correo son:

Normativa de uso de correo electrónico: Creación de un seguido de normas a la hora de usar el correo electrónico.

Antimalware y antispam: Instalación de aplicaciones para la protección contra el malware y el spam.

Ofuscar las direcciones de correo electrónico: No publicar en ninguna red social ni página web la dirección de correo electrónico de la empresa.

Uso apropiado del correo corporativo: Nunca usar el correo corporativo con fines personales.

Contraseña segura: Uso de una contraseña segura para acceder al correo.

Correos sospechosos: Si se sospecha de un correo electrónico nunca abrirlo sin antes pedir ayuda.

Identificación del remitente: Siempre saber quien es el remitente de un correo si no, no abrirlo hasta que se sepa.

Análisis de adjunto: Análisis práctico y seguro de los archivos adjuntos a los correos ya que podrían ser maliciosos.

Inspección de enlaces: Saber que los enlaces sean seguros y fiables antes de acceder o utilizarlos.

No responder al spam: Nunca contestar un spam ya que podrías dar información a alguien que no la merece.

Utilizar la copia oculta (BCC o CCO): Utilización de la copia oculta cuando envíes correos a múltiples direcciones.

Evitar las redes públicas: No consultar el correo corporativo si estás en una red pública.

Cifrado y firma digital: Instalación de cifrado y firma digital para una mayor seguridad.

Desactivar el formato HTML, la función de macros y las descargas de imágenes: Desactivación del formato HTML **,** la función de macros y la descarga de imágenes para una protección adicional.

Uso de wifi y redes externas

La empresa debe garantizar que el uso de wifi y redes externas está siendo bien realizado y es seguro.

El objetivo es establecer y difundir las buenas prácticas del wifi y las redes externas.

Los controles relativos del wifi y las redes externas son:

Política de conexión: Normativa reguladora de las conexiones externas.

Uso de la VPN: Otorgar el conocimiento de acceso vía VPN a las redes y en qué situaciones hacerlo.

Acceso a redes wifi ajenas: Al conectarte a redes ajenas tienes que comprobar que usa el protocolo WPA2 además de comprobar que es un sitio seguro y se puede navegar por él.

Redes inalámbricas de los dispositivos móviles: Utilización de redes inalámbricas y bluetooth en móvil solo cuando se vaya a utilizar.

Uso de dispositivos móviles: Revisión de las políticas de móviles en ámbito corporativo.

Uso de ordenadores no corporativos: Evitar el uso de ordenadores no corporativos y revisar la seguridad de tus dispositivos domésticos.

Configuración de la VPN: Configuración de la VPN para acceder desde el exterior con cuentas con permiso de acceso.

Configuración de la Wifi doméstica: Antes de su utilización debemos configurarlas y asegurarnos que tienen el protocolo WPA2, cambiamos el SSID y las credenciales.

Protección del puesto de trabajo

La empresa debe garantizar que el puesto de trabajo es seguro y se puede trabajar como corresponde.

El objetivo es establecer y difundir la protección del puesto de trabajo y su buen estado

Los controles relativos del puesto de trabajo son:

Normativa de protección del puesto de trabajo: Informar a todo el personal de la buena protección del puesto de trabajo y la mejor forma de mantenerlo seguro.

Sistemas operativos actualizados: Mantienes el sistema operativo actualizado y listo para el trabajo.

Antivirus actualizado y activo: El antivirus siempre tiene que estar activo y perfectamente actualizado para una buena protección.

Desactivar por defecto los puertos USB: Desactivar todos los puertos y activarlos únicamente para los empleados que necesitan dicha función.

Seguridad de impresoras y equipos auxiliares: Verificación de la protección de las impresoras y equipos auxiliares que puedan estar conectados a la red o guardando información.

Prohibición de alteración de la configuración del equipo e instalación de aplicaciones no autorizadas: Siempre que se requiera algo así avisar al personal informático y demandar un cambio de configuración o una instalación de un programa que necesites.

Política de mesas limpias: Siempre tener ordenada tu mesa sin papeles confidenciales a la vista.

Destrucción básica de documentación mediante mecanismos seguros: Utilización del destructor de papeles para la eliminación de papeles así eliminando información confidencial.

No abandonar documentación sensible en impresoras o escáneres: Recoger inmediatamente los documentos imprimidos para prevenir la malversación de estos.

No revelar información a usuarios no debidamente identificados: No revelar la información ya que podrías estar hundiendo a la empresa **.**

Obligación de confidencialidad: Aceptas y cumples la política de confidencialidad.

Uso de contraseñas: No publiques ni compartas tus claves, tampoco las notas ni otro tipo de información clave para la empresa.

Obligación de bloqueo de sesión y apagado de equipos: Cierre de todo tipo de equipos con su respectivo cierre de sesión .

Uso adecuado de internet: Conoces y aplicas la normativa del uso de internet.

Uso de portátiles y dispositivos móviles de la empresa: Conoces y aceptas la normativa de uso de la empresa para sus dispositivos portátiles y móviles .

Obligación de notificar incidentes: Notificar cualquier tipo de incidente que veas sea el tipo que sea.

Destrucción avanzada de documentación mediante mecanismos seguros: Destruyes la información de forma segura teniendo en cuenta el método apropiado.

Bloqueo programado de sesión: Programar un bloqueo automático de sesión en todos los ordenadores al no detectarse actividad.

Uso de los medios de almacenamiento: Conoces y aplicas las políticas relativas al almacenamiento seguro de la información.

Cifrado de la información confidencial: Conoces y aplicas la normativa al cifrado de información.

Conclusiones

Dados los datos mencionados en este documento, estamos convencidos de que vamos a saber como utilizar correctamente la seguridad de nuestra empresa, así como controlarla, entenderla, distribuir los conocimientos y gestionarla correctamente entre el equipo directivo, los empleados y los clientes.

Referencias

Itinerario

https://itinerarios.incibe.es/

Kit de concienciación

https://www.incibe.es/protege-tu-empresa/kit-concienciacion

Políticas de seguridad

https://www.incibe.es/protege-tu-empresa/herramientas/politicas