2021

PLAN DE SEGURIDAD

PROPUESTA DIRECTIVA

OSIX ENTERPRISE

PROPUESTA DE

EDUARD CASTELLÓ

CEO, OSIX ENTERPRISE

New Normal Life

Identificación y autenticación

Identificación y autenticación

Tarjeta de identificación

Formato de identificación de empresas	
INFORMACIÓN DEL TRABAJADOR:	
Nombre y Apellidos:	
Código:	**Puesto:**

Control de acceso

Se tendrá en cuenta un riguroso plan de control de acceso, el cual funcionará de manera escalonada, cuanto más peso tienen en la empresa más acceso tienen a esta misma.

Lo único que no seguirá esta norma es el acceso a empleados que requieran un acceso especial para realizar su trabajo o requiera de ello por una orden o necesidad. (se le otorgará la tarjeta necesaria durante un periodo de tiempo)

Todo esto con unas cerraduras electrónicas y unas tarjetas para abrir las puertas y controlar el acceso de la empresa.

Registro de acceso

El registro de acceso se basará en un riguroso documento el cual se basará en:

Nombre: Eduarda
Apellidos: Castellana Lana
DNI: 48297815A
Puesto de trabajo: “”
Dia de inicio: 12/02/2021
Dia de hoy: 12/02/2021
Número de trabajador: “1”

Acceso a datos

El acceso a datos funcionaria de forma similar que el control de acceso, ya que se tendrá muy en cuenta quién tiene acceso a según qué datos, y se seguirá una jerarquía de importancia empresarial para la obtención de datos de la empresa.

De todas formas también se requerirá de una supervisión mensual de los datos que hayan sido supervisados y sobretodo por quien.

Esto se logra gracias a controles de acceso en todos los informes y diferentes niveles de seguridad en estos mismos.

Como clave final también se deberá avisar a su supervisor antes de acceder a esos datos, sobretodo si tienes permisos limitados.

En cada puesto donde se sitúa un ordenador abra una cámara insertada en la zona la cual se asegure de registrar quien entra en ese ordenador y a que hora.

Copias de Seguridad

PROTECTED BY
OSIX ENTERPRISE

Copias de seguridad e imágenes del sistema

En este tema de las copias de seguridad e imágenes del sistema podríamos tener a una empresa subcontratada para hacer el mantenimiento de los ordenadores y también para hacer las copias de seguridad , o sino con los servidores podríamos crear una base de datos para ir haciendo las copias de seguridad en la nube.

Sistema de redundancia

Este respaldo es básicamente para la red que utiliza tu proveedor de Web Hosting para mantener tu información en línea. Las compañías fiables tienen más de un operador de internet para el funcionamiento de sus servidores de modo de garantizar que tu sitio web nunca estará abajo por la interrupción de un enlace de red.

Mantener esto significa tener una inversión para mantener los servidores y tener varias líneas de internet para no tener nunca una caída de los servidores.

También hay una parte de la redundancia que se refiere a las piezas físicas de hardware del servidor. Por ejemplo, una capa de redundancia es para los discos duros. La idea es, si llegara a fallar un disco duro en un servidor, este se mantenga en funcionamiento y tu sitio no deje de estar en línea, a través de arreglos RAID en el servidor, se cuenta con repuestos de emergencia que permiten la continuidad de funcionamiento.

En esta parte anteriormente explicada hace falta hacer una inversión de manera previa antes de crear nada en la parte de hardware para no tener componentes que hagan que el servidor se pueda caer o que al llevar 40h encendido haga que se rompa o cualquier otra cosa , ya que esto haría que a la empresa le creará pérdidas de dinero importantes y esto no le tendría que interesar.

A el sistema de redundancia le tendríamos que dedicar unos 300€/mes o tener algún trabajador especializado en realizar estas tareas.

Discos duros

Este es un apartado importante para la empresa ya que será donde se almacenará toda la información de la empresa.

Primeramente tendremos el guardado en la nube de toda la información que manejan nuestros trabajadores también para tenerlo todo protegido , pero también tendríamos una red local de almacenamiento en local con centros de

almacenamiento como el siguiente de 20 TB cada uno, aumentables a 24 y/o 28 si en algún momento se necesitará.

https://shop.westerndigital.com/es-es/products/external-drives/wd-my-book-duo-usb-3-1-hdd?utm_medium=pdsh2&utm_source=gads&utm_campaign=WD-EU-ES-PLA&utm_content=895040615489&utm_term=WDBFBE0200JBK-EESN#WDBFBE0200JBK-EESN

En total para almacenar toda la información en local y tener una copia física de los documentos y tenerlos controlados hemos calculado que podría ascender a unos 3.360€. incluyendo únicamente el guardado en local , el guardado en la nube tendría otro precio juntamente con el presupuesto de seguridad y el precio de los servidores y su montaje y mantenimiento.

CPD y DRS

Proporcionamos un CPD, también denominado como Centro de Procesamiento de Datos, que es un espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización, para asegurar la continuación de sus funcionalidades y un DRS o plan de contingencia que es un instrumento de gestión para el manejo de las TIC, contiene las medidas técnicas humanas y organizativas necesarias para una organización, elaborado por nuestra empresa, para garantizar la máxima seguridad de la información.

Personal and security

PROTECTED BY
OSIX ENTERPRISE

Personal y seguridad

Como personal de seguridad y la propia seguridad de la empresa, New Normal Life contará con tres distintas catalogaciones para tener mayor efectividad y seguridad.
Tendremos planteadas 3 diferentes políticas y planes para poder ocupar todos los sectores referentes NNL y sus empresas importadoras y exportadoras, tendremos además la facilidad de contentar a nuestros clientes con unas políticas firmes, claras, fáciles y seguras, que les podremos demostrar en todo momento.
Estos documentos serán divididos y catalogados por puntos para la clara interpretación y la facil sustitucion y reparacion de los diferentes fallos que puedan surgir.
En este documento también se tiene en cuenta la seguridad del propio establecimiento de compra, de los clientes dentro de la misma y de los productos a la venta, dando diversas opciones para la vigilancia y seguridad del local de ventas.

Personal de seguridad

El personal de seguridad será el encargado de garantizar la seguridad de todo lo referido a las sucursales de venta que tenga New Normal Life, por lo tanto deberán tener la suficiente habilidad como para:

- Identificar posibles amenazas en horas de apertura
- Ser capaz de prever clientes que tengan como objetivo el posible hurto
- Poder expulsar a los clientes conflictivos de la tienda, sin causar muchos revuelos.
- Poder tener la capacidad de solucionar conflictos sin que suponga un peligro para todas las personas
- Poder controlar un número elevado de clientes sin que ninguno suponga un problema
- Acudir rápida y efectivamente a cualquier disputa

En este punto se ha decidido proponer varios presupuestos más o menos económicos, dependiendo de las seguridad que desee, estas propuestas están detalladas en el documento excel llamado “Presupuesto de personal”.

Plan de personal de seguridad extremo

Pablo García, 39 años, ex-policía retirado con 13 años de experiencia, capaz de realizar todas las habilidades pertinentes en este sector.

Sergio Perez, 26 años, personal de seguridad privado con 4 años de experiencia, capaz de realizar todas las habilidades pertinentes en este sector.

Marc Ramón, 46 años, ex-militar retirado con 8 años de experiencia, ex-personal de seguridad durante 3 años, capaz de realizar todas las habilidades pertinentes en este sector.

Julian Sans, 23 años, guardaespaldas desde hace 4 años, capaz de realizar todas las habilidades pertinentes en este sector.

Plan de personal de seguridad intermedio

Will Sanchez, 28 años, Guardaespaldas privado con 2 años de experiencia, capaz de realizar varias habilidades pertinentes en este sector.

Petrov Kirat, 31 años, ex-militante de la Unión Soviética, capaz de realizar todas las habilidades pertinentes en este sector pero no entiende muy bien el español.

Plan de personal de seguridad bajo

Eduarda Castellana, 20 años, tiene el bachillerato de artes y quiere un trabajo en el que ganar dinero fácil, puede realizar algunas habilidades de las que se requieren.

Política de seguridad

Como seguridad establecida en la empresa, hemos formalizado un extenso documento detallando cada apartado y acción a seguir para tener una seguridad eficiente para la compañía, incluida la empresa, los empleados, los proveedores e incluso los clientes. se detallan las acciones, las medidas necesarias y los documentos que son necesarios.

Los objetos estarán adjuntos en la carpeta “presupuesto política de seguridad” con varios archivos pdf para tener en cuenta el precio de cada implementación y el total de los mismos.

En este apartado de personal y seguridad solamente se presentará un documento final y no varios tipos de presupuestos, ya que pensamos que es muy necesario tener la seguridad mínima en políticas de seguridad, y eso será lo que ofreceremos.

El documento general de las políticas necesarias está formalizado en el archivo “políticas de seguridad” adjuntado también a estos documentos.

Plan de contingencia

Para poder realizar el plan de contingencia correctamente, primero deberemos saber qué recursos tiene NNL y organizarlos según la prioridad que deseemos.

Para ese documento se tendrá en cuenta que el recurso principal y más prioritario de NNL, son las opiniones y los datos de los clientes y proveedores.

Se deberán identificar los riesgos clave de la empresa, para ello los empleados son una parte fundamental, es necesario que sean conscientes de los riesgos que corren al realizar cada acción y como arremeter contra los problemas para solucionarlos eficazmente.Estos riesgos también deben de ser organizados según su prioridad.

El plan de contingencia empieza catalogando los recursos de NNL según su prioridad:

- Datos de NNL
- Datos de los clientes y proveedores
- Datos del personal contratado
- Datos de los productos de NNL
- Personal contratado
- Clientes
- Hardware de la sucursal de NNL

Seguidamente tendremos una lista de los riesgos organizados según su prioridad:

- Robo de información confidencial de NNL
- Robo de información privada de NNL
- Robo de información de clientes y empleados
- Agresiones físicas de clientes a empleados o de empleados a clientes
- Agresiones a la tienda física de NNL
- Rotura de material de hardware propiedad de NNL

Una vez obtenido los puntos clave de los recursos y riesgos de NNL, las contingencias a seguir para cada problema están detallados a continuación:

Una vez la empresa ha recibido un ataque de robo de información de cualquier tipo, se procederá a verificar y diagnosticar cuando y como a podido suceder ese error, una vez hecho el diagnóstico, se procederá a establecer los parques necesarios para no ir perdiendo más datos, establecido el parche, detectaremos al culpable del robo y se procederá de la forma mas beneficiente para NNL, ya sea contactando con las autoridades y denunciando o hablando directamente con el culpable y después de ello, probaremos y mejoramos el parche establecido para asegurarnos de que no volviera a pasar.

Conforme el punto de contingencia para las agresiones físicas, la única opción racional a seguir, sería:

- Si un empleado es agredido se procede a sacar al agresor fuera de la tienda gracias a la seguridad de NNL y llamar a las autoridades para denunciar la agresión. Exactamente, se seguirá el mismo proceso si un cliente rompe intencionadamente algún producto de la tienda.

- Si un empleado agrede a un cliente, se procederá al despido del mismo, también se le darán las facilidades que el cliente necesite si este desea denunciar al empleado.

Protección de datos

La protección de datos de NNL contendrá un sistema de cifrado para cada uno de los envíos de información, ya sea entre empleados en la empresa o modificaciones en las bases de datos o servidores, todos los dispositivos empresariales contará con el sistema de cifrado WPA2 para maximizar la protección de absolutamente todos los datos.

Contaremos también con un sistema de seguridad con nuestros proveedores, teniendo asi documentos con nuestros requerimientos según la seguridad que queramos establecer con los proveedores, a parte de varios contratos de confidencialidad para asegurar que nuestros datos no son difundidos.

Respecto a un tema de ciberseguridad, nuestros expertos configuraron una red segura con varios firewalls y niveles de seguridad para evitar ciberataques y robos de datos.

Para evitar los robos de información todos los empleados recibirán un curso sobre la seguridad que deben tener al trabajar con NNL, al no cumplir las normas enseñadas se podría proceder al despido inmediato del trabajador.

Seguridad Física Lógica Redes

PROTECTED BY
OSIX ENTERPRISE

Seguridad física

La seguridad física es un conjunto de mecanismos concebidos para detectar amenazas físicas al hardware. Nuestra empresa aporta uso de cámaras de videovigilancia, sistemas SAI para evitar que un apagón impida la realización de las funciones de la empresa, contratación de una segunda empresa conexión para garantizar absoluta disponibilidad de la red y de los equipos, subcontratación de una empresa de seguridad privada para la vigilancia del uso de los equipos y espacio de trabajo. Además ventanas de espejo de seguridad laminado, para evitar que la gente pueda espiar desde el exterior.

Seguridad lógica

La seguridad lógica la conforman todas aquellas barreras que evitan, virus, programas no testeados y accesos no autorizados entre otros, Osix aportaría cámaras de videovigilancia para comprobar que haya un correcto uso de los equipos, antivirus con eficacia testada y asegurada por nuestra empresa, un documento de concienciación para la seguridad de la empresa.

Seguridad en las redes

La seguridad en las redes consiste en las políticas y prácticas adoptadas para prevenir y supervisar el acceso no autorizado, el uso indebido, la modificación o la denegación de una red informática y sus recursos accesibles. Para ello el uso de programario de control de paquetes de red para evitar conexiones a sitios no deseados en la empresa, uso de vpn local para garantizar máxima velocidad en comunicaciones internas de la empresa.