Este documento debe ser utilizado como plantilla base para la elaboración de los planes de recuperación de entornos. Se entiende entorno como un conjunto de equipos, dispositivos, y aplicaciones que son concebidos como una entidad con una misma finalidad. En ocasiones, un entorno será una aplicación, y en otros casos un conjunto amplio de dispositivos.

Por ejemplo, el correo electrónico puede ser considerado un entorno, al igual que una aplicación de facturación, con independencia de los sistemas que compongan ambos.

Este tipo de documentos se encuentran a mitad camino entre el Plan de Crisis y las instrucciones técnicas de trabajo.

Cada uno de los apartados contiene información específica cómo cumplimentarlo.

PLAN DE RECUPERACIÓN DE ENTORNO

<< *NOMBRE DEL ENTORNO* >>

Datos del Documento

Alcance y descripción

Describir los escenarios de contingencia a los que se hace frente este documento.

Propietario del documento

Persona responsable del Plan. Esta es la persona responsable de que el documento se mantenga actualizado y sea revisado de manera periódica.

Histórico de versiones

Cada vez que se revise o modifique el documento, tiene que reflejarse en la tabla inferior, incluso cuando se revisa pero no se modifica.

Fecha	Autor	Descripción

Elementos del plan

Infraestructura TIC

Incluir la lista de activos TIC relacionados con el entorno objeto de recuperación. En general, deben incluirse los detalles suficientes para identificar el equipo sin ningún género de duda.

No es necesario que aparezcan direcciones IP o detalles técnicos, excepto si no hay otra forma de identificación.

Personal técnico

Incluir los contactos del personal técnico competente para la ejecución de este Plan de Recuperación. Esto incluye nombres y datos de contacto: teléfonos y correo electrónico.

Proveedores

Incluir los contactos de los proveedores con los que se han establecido contratos de mantenimiento y/o pueden prestar soporte en la ejecución de este Plan de Recuperación.

Esto incluye nombres de personas y datos de contacto: teléfonos y correo electrónico.

Ejecución del Plan

Acciones

A continuación se deben describir paso por paso las acciones necesarias para recuperar el entorno.

El detalle técnico que se desee incluir queda a criterio del usuario, y dependerá mucho de la complejidad del procedimiento en cuestión.

Lo mejor es que este documento refleje los pasos principales y referencie a procedimientos más técnicos y específicos que puedan ser actualizados con mayor frecuencia sin que el núcleo del plan cambie demasiado a menudo.

A continuación se muestra un ejemplo de lo que sería un plan de recuperación para la caída de un nodo de entrada a un entorno por donde acceden los proveedores:

Paso	T	Acción	Información, recursos y comentarios
1	0m	Identificar los proveedores que acceden a través del nodo caído Ver paso siguiente	Ver el listado de proveedores por punto de entrada. El nodo caído puede ser: • Telco1 • Telco2
2	10m	Acceder al concentrador de túneles que actúa en el extremo caído. Abrir una conexión simultánea en el concentrador de túneles que actúa en el extremo alternativo.	En el caso de caída de Telco1, el concentrador de túneles corresponde a los firewall Cisco. En el caso de caída de Telco2, el concentrador de túneles corresponde a los firewall Netgear. Ver procedimiento de acceso a los firewalls.
3	25m	Para cada conexión VPN existente en el nodo caído: 1. Comprobar si existe una conexión VPN creada en el nodo alternativo. 2. Si existe, verificar que los parámetros de ambas conexiones son iguales o equivalentes.	Estas conexiones pueden estar ya creadas, aunque deben verificarse los parámetros de conexión. Ver procedimiento de obtención de VPNs y parámetros de conexión.
4	50m	Para aquellas conexiones VPN existentes en el nodo caído que no estén creadas en el nodo alternativo,	Ver procedimiento de creación de VPN en el firewall Netgear.

Paso	T	Acción	Información, recursos y comentarios
		crear una VPN Lan2Lan en el nodo alternativo con los mismos parámetros de configuración que la red original.	Ver procedimiento de creación de VPN en el firewall CISCO ASA.
5	60m	Por orden de importancia y volumen de negocio, notificar a cada proveedor identificado en el punto 1 la nueva IP pública a la que debe conectarse vía VPN.	Ver listado de proveedores por punto de entrada. Ver datos de contacto de proveedores. Ver IP pública de Telco1 para el concentrador Cisco ASA. Ver IP pública de Telco2 para el concentrador Netgear.
6	75m	El proveedor deberá modificar la IP de conexión a la VPN en su router o firewall.	Tras la modificación, el proveedor debe intentar conectar a un equipo interno que use habitualmente, forzando a que el túnel se levante.
7	100m	Verificar que la conexión entre extremos es correcta. FIN DEL PLAN	Ver procedimiento de identificación de estado en routers y concentradores VPN.