

1.- PROPÓSITO

La gestión de la información empresarial se realiza fundamentalmente desde el puesto de trabajo, tanto desde dispositivos tecnológicos como de forma más tradicional (papel, teléfono, ETC). De ahí la importancia de que los trabajadores y las trabajadoras se conciencien y se responsabilicen del cumplimiento de ciertas normas para la seguridad en, y desde, su puesto.

Por una parte, deben conocer los riesgos no tecnológicos, por ejemplo:

- información en papel al alcance de personas no autorizadas;
- la falta de confidencialidad de los medios de comunicación tradicionales;
- el peligro de robo o extravío de los dispositivos extraíbles (pendrives, discos duros externos, etc.);
- el acceso físico de terceras personas a las zonas de trabajo (repartidores, personal de limpieza, etc.).

Por otra parte, desde muchos puestos de trabajo se tiene acceso a ordenadores, dispositivos móviles y portátiles con conexión a la red de la empresa y al exterior (internet). Son pues una «puerta de entrada» a la entidad y a sus recursos de información. Es esencial que toda la plantilla tenga conciencia de lo que esto implica, a fin de evitar incidentes que puedan iniciarse en su puesto de trabajo, y agravarse por desconocimiento o por falta de cuidado:

- accesos no autorizados a los ordenadores y desde ellos a aplicativos de la empresa;
- infecciones por malware;
- robo y fuga de datos en formato digital;
- ataques de ingeniería social, es decir, engaños para manipular a la víctima para obtener información (credenciales, información confidencial o conseguir que realice alguna acción por él (instalar un programa, enviar algunos correos, hacer algún ingreso, etc.).

Para garantizar un uso adecuado de los dispositivos y medios del entorno de trabajo, y minimizar el impacto que todos estos riesgos pueden tener en la empresa, debe implantarse una política de protección del puesto de trabajo. A continuación, se detallan una serie de obligaciones y buenas prácticas en materia de seguridad para aplicar en el puesto de trabajo, con el objetivo de garantizar la seguridad de toda la información y los recursos gestionados desde el puesto de trabajo.

1.- ALCANCE

La presente política es aplicable a:

Todas las personas que intervengan en los sistemas de procesamiento de datos personales de Patronato Intermunicipal Francisco Esteve y que pertenezcan a los siguientes PERFILES: Administración; Gerencia; Direcciones Técnicas; Personal de Atención Directa, Responsable de Mantenimiento e Infraestructuras.

3.- OBLIGACIONES Y BUENAS PRÁCTICAS PARA APLICAR**3.1- DESTRUCCIÓN DE DOCUMENTACIÓN**

La información confidencial obsoleta o que ya no sea útil debe ser destruida de forma segura.

La información obsoleta se destruirá de forma segura según la política de borrado seguro y gestión de soportes. En particular:

- mediante destructoras de papel al servicio de los empleados;
- contratando un servicio externo de destrucción segura, notificando a los empleados de su existencia y obligación de uso;
- dando a conocer los riesgos asociados a la utilización de papeleras para documentos sensibles (datos personales, información financiera, etc.).

3.2- BLOQUEO PROGRAMADO DE SESIÓN

Se debe programar el bloqueo automático de sesión en los equipos al no detectarse actividad del usuario durante un corto (máx.15 min)

El personal informático programará un bloqueo automático de sesión en los equipos al no detectarse actividad del usuario en un corto periodo de tiempo.

3.3- SISTEMA OPERATIVO ACTUALIZADO

Se deben mantener actualizados los sistemas operativos de los equipos informáticos. El personal responsable de los sistemas aplicará la política de actualizaciones de software revisando los equipos periódicamente.

3.4- ANTIVIRUS ACTUALIZADO Y ACTIVO

Se debe mantener al antivirus actualizado y activo en todos los equipos informáticos. El personal responsable del mantenimiento de los sistemas informáticos aplicará la política antimalware que incluye la instalación y actualización de las herramientas antimalware en todos los equipos y sistemas y realizará la revisión periódica de manera que se garantice la protección ante ataques con malware.

3.5- USO DE MEDIOS DE ALMACENAMIENTO

La información debe ser almacenada en dispositivos autorizados y de forma segura. Por ejemplo, los dispositivos externos como pendrives o discos duros deben ser encriptados.

3.6- PROHIBICIÓN DE ALTERACIÓN

No está permitido alterar la configuración del equipo o instalar aplicaciones no autorizadas. Siempre debe solicitarse al personal informático la instalación de software específico o el cambio de configuración del equipo si es necesario para el desempeño del trabajo.

3.7- POLÍTICA DE MESAS LIMPIAS

Las mesas de trabajo deben encontrarse siempre despejadas y sin documentación confidencial ni dispositivos extraíbles al alcance de otras personas.

Conocemos como política de mesas limpias la obligación de guardar la documentación de trabajo al ausentarse del puesto de trabajo y al terminar la jornada laboral. No se debe dejar información sensible a la vista de personas que pudieran hacer un uso indebido de la misma. El cumplimiento de esta política conlleva:

- mantener el puesto de trabajo limpio y ordenado;
- guardar la documentación y los dispositivos extraíbles que no están siendo usados en ese momento, y especialmente al ausentarnos del puesto o al fin de la jornada laboral;
- no apuntar usuarios y contraseñas en post-it o similares

3.8- CUSTODIA DE LA DOCUMENTACIÓN SENSIBLE.

Se debe recoger inmediatamente aquellos documentos enviados a imprimir y guardar la información una vez escaneada,

Los archivos, armarios, almacenes o despachos que contengan documentación o información sensible deben estar protegidos con llave y se debe disponer de una relación de personal que dispone de esa llave. No se debe dejar la llave puesta cuando se esté ausente.

El personal debe asegurarse de que no queden abiertas las puertas de acceso a la calle bajo ningún concepto. Esto puede facilitar una intrusión de personas no autorizadas y poner en riesgo la seguridad.

3.9- CONTRASEÑAS

Se debe seguir la Política de Contraseñas:

- las credenciales (usuario y contraseña) son confidenciales y no pueden ser publicadas ni compartidas;
- no deben anotarse las credenciales en documentos ni en cualquier otro tipo de soporte;
- las contraseñas deben ser robustas: al menos 8 caracteres incluyendo mayúsculas, minúsculas, números y caracteres especiales (!, @, +,], ?, etc.);
- Se recomienda el cambio periódico de contraseñas (p.e cada seis meses)

3.10- BLOQUEO DE SESIÓN Y APAGADO DE EQUIPO

Es obligatorio bloquear la sesión al ausentarse del puesto de trabajo y apagar el equipo al finalizar la jornada laboral.

3.11- NOTIFICACIÓN DE INCIDENTES

Es obligatorio notificar cualquier incidencia de seguridad (virus, pérdida de información o de dispositivos, etc.)

El/la trabajador/a debe advertir de cualquier incidente relacionado con su puesto de trabajo:

- alertas de virus/malware generados por el antivirus;
- llamadas sospechosas recibidas pidiendo información sensible;

- correos electrónicos que contengan virus;
- pérdida de dispositivos móviles (portátiles, smartphones o tabletas) y dispositivos externos de almacenamiento (USB, CD/DVD, etc.);
- borrado accidental de información;
- alteración accidental de datos o registros en las aplicaciones con información crítica; comportamientos anómalos de los sistemas de información;
- hallazgo de información en ubicaciones no designadas para ello;
- evidencia o sospecha de acceso físico de personal no autorizado, a áreas de acceso restringido (CPD, despachos, almacenes...);
- evidencia o sospecha de accesos no autorizados a sistemas informáticos o información confidencial por parte de terceros;
- Cualquier actividad sospechosa que pueda detectar en su puesto de trabajo.

Fdo. Gerencia

EVA
MARIA|
LUNA|
BOTET

Firmado
digitalmente
por EVA MARIA|
LUNA|BOTET
Fecha:
2023.02.09
16:22:39 +01'00'